Raju & The Forty Thieves

A Booklet on Modus Operandi of Financial Fraudsters

Office of the RBI Ombudsman (Mumbai-II)
Maharashtra And Goa

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

Foreword

As a part of the Reserve Bank of India's customer awareness initiatives, in July 2021 this office had published a booklet 'Be(A)ware' on the modus operandi of financial fraudsters. Encouraged by the positive response received from members of the public as well as different institutions, we take forward the idea of financial education, to be more accessible to those who have just begun their journey into digital financial world and are not so well-versed with the nuances of online financial transactions. This includes people from different ages and education levels such as school children, young adults, semi-literates and senior citizens, irrespective of whether they live in urban, rural or semi urban areas.

Continuing the 'Be(A)ware' series, this booklet 'Raju and the Forty Thieves' is a manifestation of our efforts. The booklet is an easily understandable pictorial depiction of incidents happening around us and helps us to learn how to keep hard-earned money and ourselves safe from fraudsters.

As the name suggests, 'Raju and the Forty Thieves' contains forty such stories providing glimpses of fraudulent events being reported to us and provides simple tips about DOs and DON'Ts. Raju is a typical gullible citizen, and, in these stories, he appears in different characters, some time as a senior citizen, some time as a farmer, sometimes as a happy-go-lucky guy, etc., although with same curly hair always to identify with different walks of life.

Let us make ourselves aware of such modus operandi used by fraudsters and educate those around us to be aware of such financial frauds. The tireless efforts put by the team of RBI Ombudsman, Mumbai-II, Maharashtra and Goa, to spread financial literacy by preparing such booklets during covid period, is gratefully acknowledged.

The readers are requested to share their feedback and suggestions, if any, to bomumbai2@rbi.org.in.

Be Aware and Beware!

INDEX

Don'ts:

× Don't click on unknown/unsolicited links received on the phone/email without verifying it.

× Don't share your confidential details with strangers.

2. VISHING CALLS

Do's:

- ✓ Always cross-check with your relationship manager or bank branch about any issue before trusting anyone.
- ✓ OTP is like a key to your safe wealth, so always keep it away from fraudsters.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in

Don'ts:

- Don't trust unknown callers claiming to be speaking on behalf of banks asking for confidential information / details. Banks don't seek such details over phone.
- Never trust strangers in the digital world easily, and be cautious while answering calls from unknown numbers.

3. FRAUD USING ONLINE MARKETPLACES

Do's:

- Always remember, UPI PIN is required only to make a payment and is not required to receive any payment.
- Always verify the mobile number in the UPI application before initiating a payment.
- Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in

Don'ts:

- × **Don't share OTP or confidential account details with strangers.**
- × **Don't enter the UPI PIN to receive an amount from another person.**

4. CREDIT CARD ANNUAL FEE WAIVER- FAKE OFFER

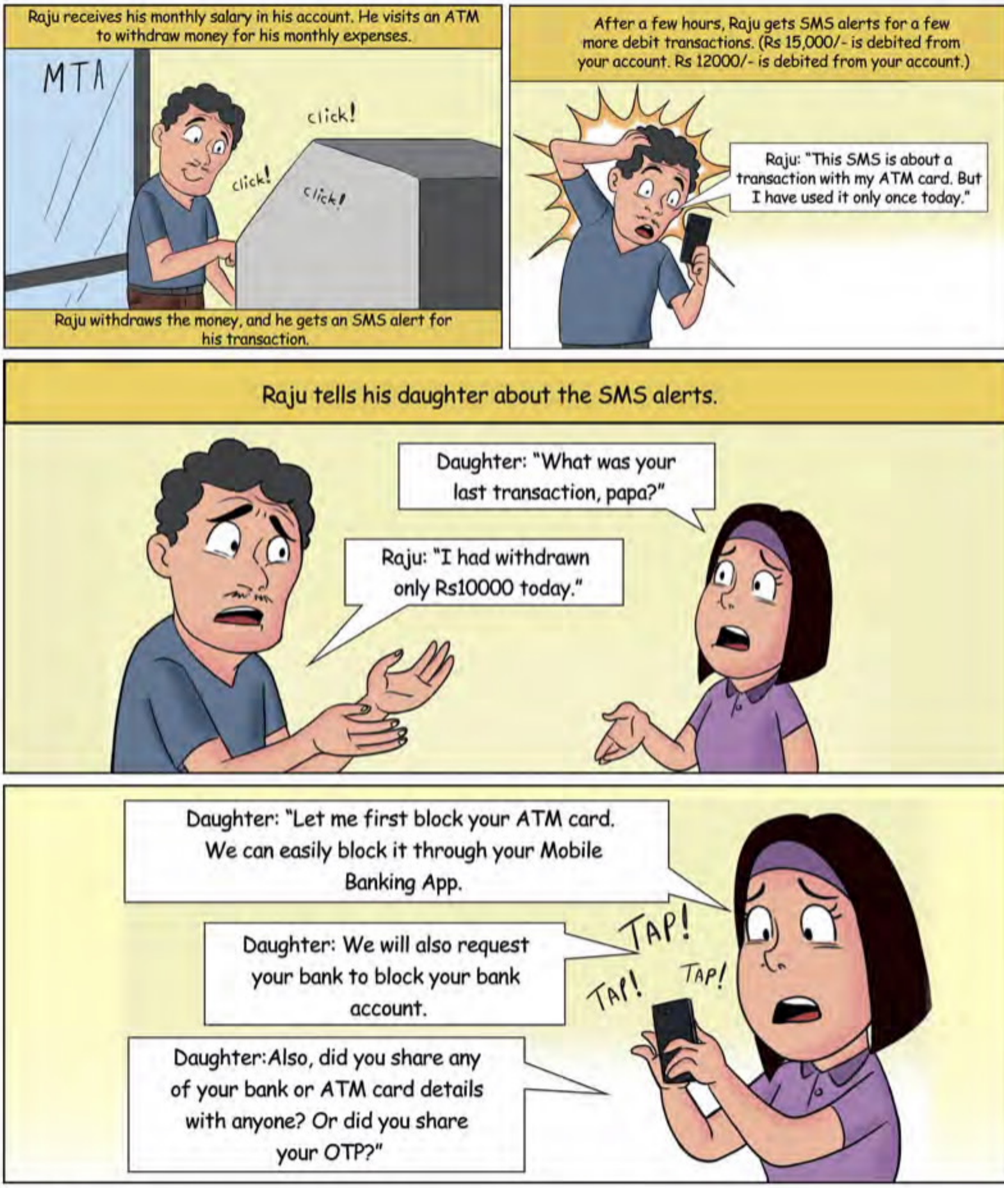
Do's:

- ✓ Be cautious while responding to calls from unknown numbers claiming to be from your bank.
- ✓ Report to your Homebranch immediately on realizing the fraud.
- ✓ Block your card to prevent further financial loss.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in

Don'ts:

× **Don't share your OTP with anyone. Fraudsters might be able to collect your account details, but transactions can only happen if you share the confidential OTP sent to your phone.**

5. ATM CARD SKIMMING FRAUD



Do's:

- Before initiating any transaction in the ATM machines, ensure that skimming devices are not present. Skimming devices are hidden by fraudsters by overlapping them with the card insertion slot.
- Report the fraud to the bank within 3 days of the card cloning incident.Check your transaction history frequently to verify all transactions.
- Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at (https://cybercrime.gov.in)

Don'ts:

- ✗ Don't give your ATM card to anyone on the ATM premises to transact on your behalf. This kind of social engineering is being used to target senior citizens/semi-educated persons who have difficulty operating ATMs.

6. FRAUD USING SCREEN SHARING APP/REMOTE ACCESS

Do's:

- Verify the authenticity of the offer on the official website of the entity concerned.
- Install antivirus/spam blocking software on your mobile phone.
- Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in

Don'ts:

- × Don't download any applications over links sent through SMS, Email or instant messaging applications.
- × Don't download screen-sharing applications shared by any unknown persons.
  Screen sharing codes generated by these apps should not be shared with unknown persons.

7. SIM SWAP/ SIM CLONING

Do's:

- Verify the status of the SIM card with your Telecom Service Provider when in doubt instead of believing unknown callers.
- Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in

Don'ts:

× Don't share confidential details like Aadhaar number and SIM number with unknown callers.

Don'ts:

- Don't contact random phone numbers obtained from web search engines, especially for doing financial translation.

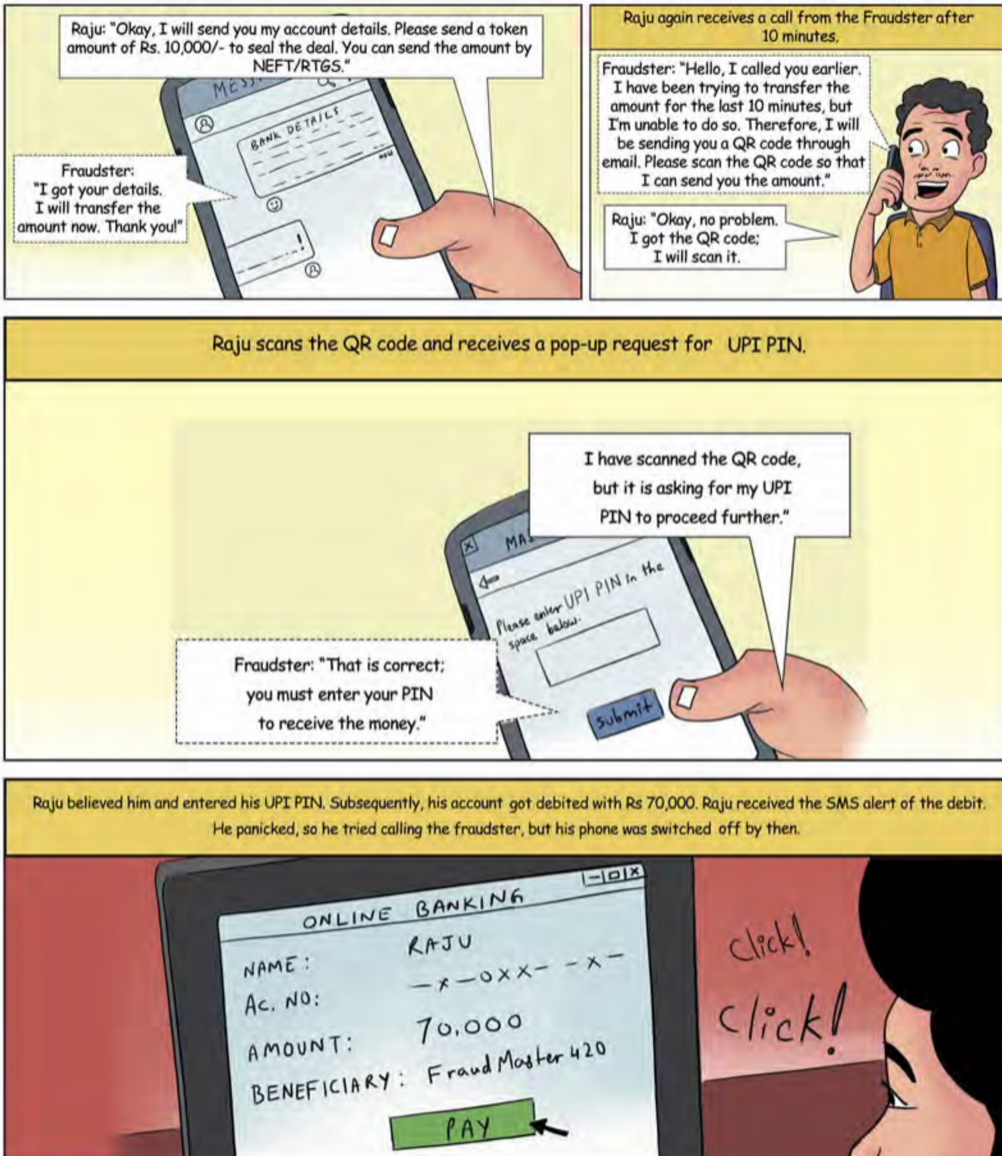
9. SCAM THROUGH QR CODE SCAN

Raju registered his old car on an online website to sell it.

Within hours, he was contacted by a person (a fraudster)

Do's:

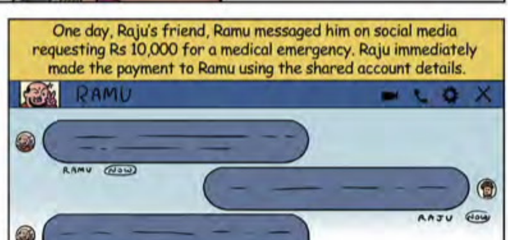
- ✔ Educate yourself about QR codes before using them.
- ✔ Report the transaction immediately to your bank.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in



Don'ts:

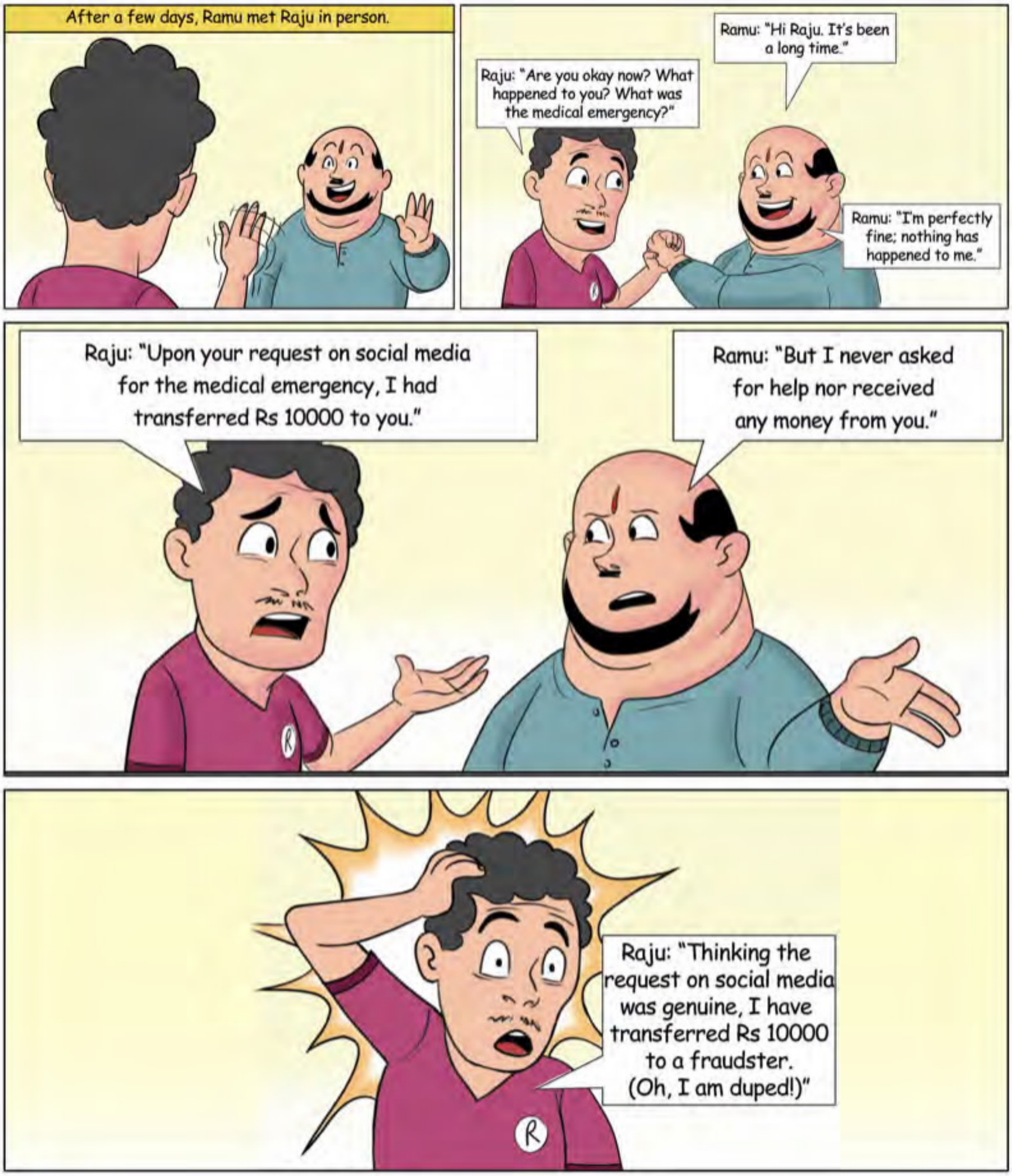
- × Don't enter your UPI PIN to receive money from another person. UPI PIN is required only for sending a payment, not for receiving.
- × Don't scan QR codes to receive any payment. QR code needs to be scanned for sending a payment, not for receiving Money.

10. IMPERSONATION THROUGH SOCIAL MEDIA



Do's:

- ✔ Verify by calling/meeting the real person before making a payment.
- ✔ Always check the account details before making any payment.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in



Don'ts:

- Don't keep your personal information like mobile number, email id and friend list open to the public.
- Don't accept friend requests/ follow requests from people you have never met in person.

11. JUICE JACKING – STEALING OF DATA THROUGH CHARGING CABLE

Do's

- ✓ Install anti-virus software on your mobile phone to protect it from unauthorized access.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in

Don'ts:

× Don't use charging adapters/cables from strangers.

Don'ts:

- Do not make payments without verification, expecting very high returns.

13. ONLINE JOB FRAUD

Do's:

- ✓ Verify the authenticity of the company or recruitment agencies before paying any money. Recruitment agencies generally do not charge candidates for hiring them.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in

Don'ts:

× Don't pay anyone under the pretext of a job. A legitimate company will never ask for payment from a potential candidate for a job offer.

Don'ts:

× Do not pay anybody without verifying the authenticity of the company.

15. FRAUD THROUGH EMAIL

Do's:

- ✓ Verify with the person concerned before making any payment based on the email received.
- ✓ Verify the email ID.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in

Don'ts:

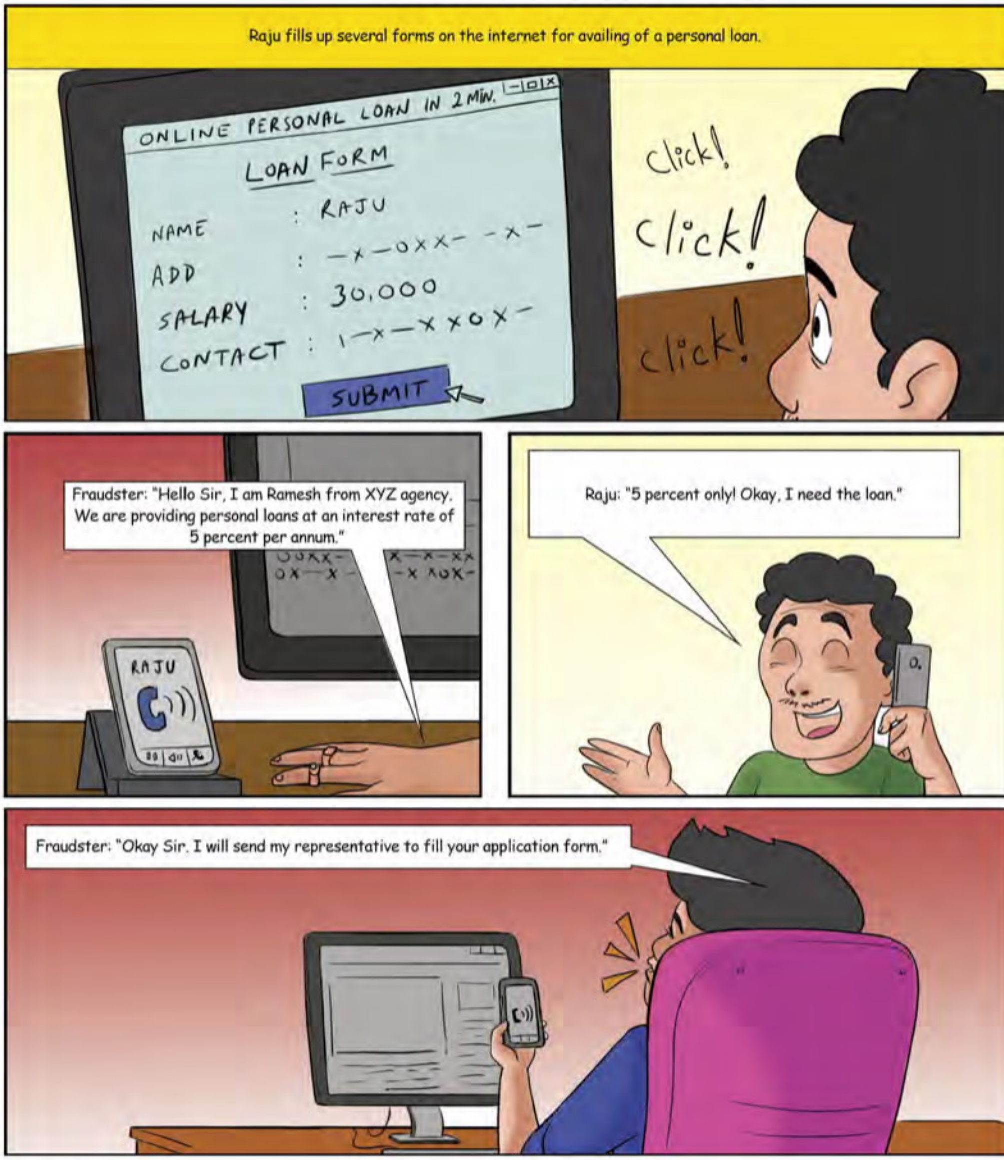
✕ Don't make payments on receiving requests from random emails or similar-looking email ids.

Don'ts:

× Don't trust unknown callers offering easy banking services and sending texts through Messaging Apps.

× Don't share card details and OTP.

17. FRAUDULENT LOANS WITH STOLEN DOCUMENTS

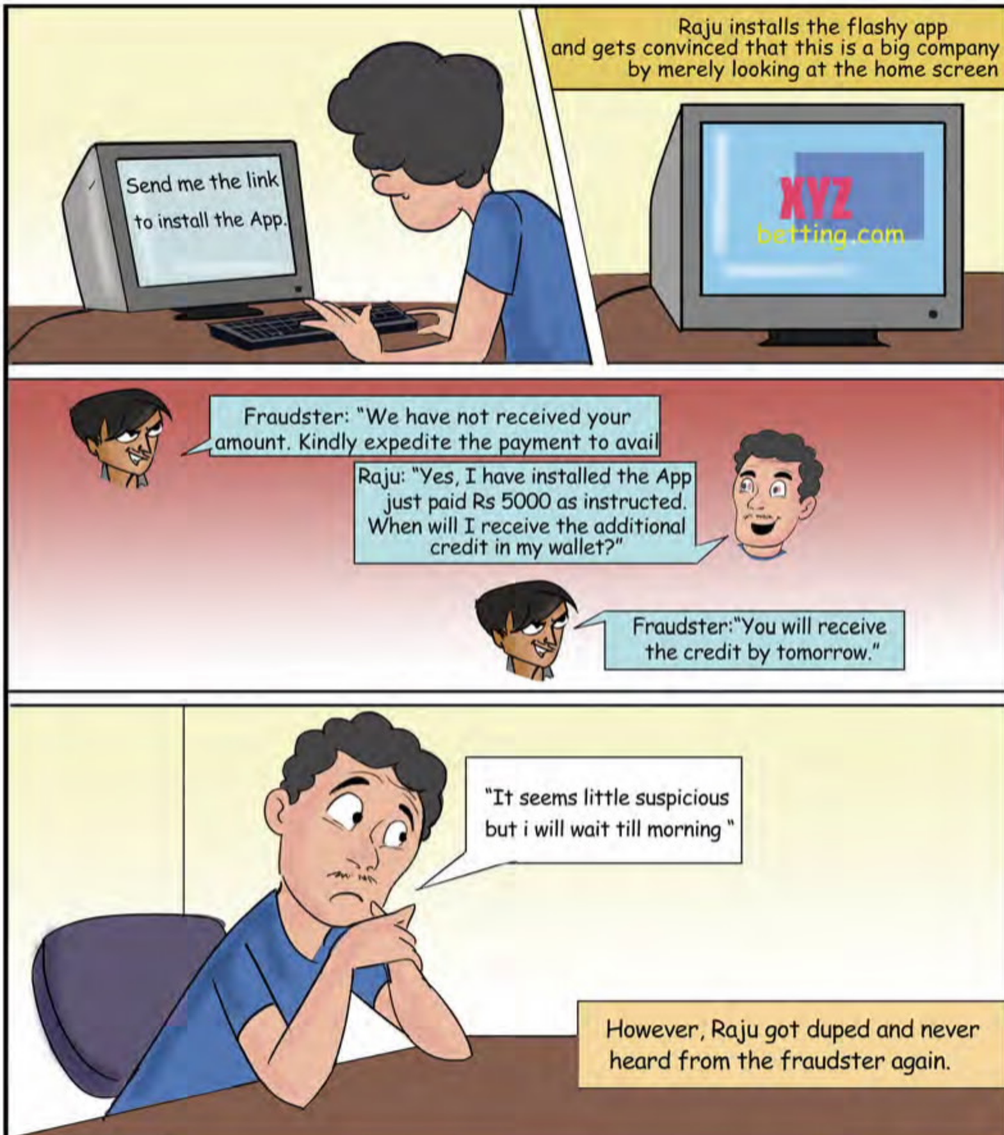


Do's:

- ✔ Always monitor the end-use of the documents in the transactions.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in

Don'ts:

✕ Never share your confidential details like the Aadhaar number, PAN number, cheque book or cheques with unknown persons.



Don'ts:

× One should not make payments on unknown websites.

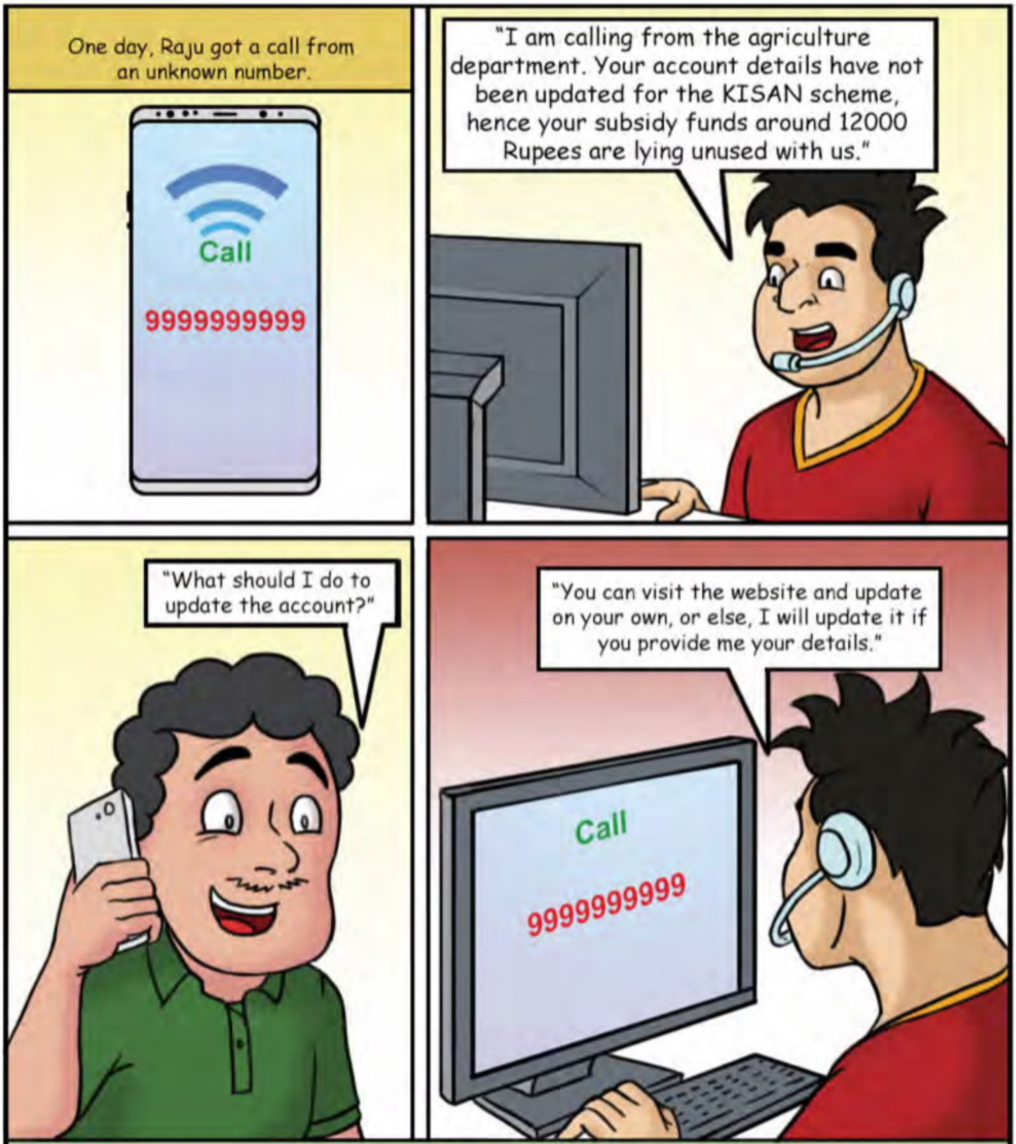
19. FAKE VACCINATION CALL

Do's:

- ✓ Read the entire SMS to read the purpose of OTP.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.


Thereafter, the person disconnected the call and switched off his number.
221178725
Raju got tensed, and he searched the helpline number on the ABC Diagnostics site but couldn't find it.
ABC Diagnostics
couldn't find it
Raju eventually realized he was defrauded.
Don'ts:
✕ Do not make a payment in advance when you are doubtful. If anybody asks for an advance payment,it is a matter of caution
and one should go ahead with those transactions with requisite precaution.

22. SOCIAL WELFARE SCHEME FRAUD



Do's:

- ✔ Verify the details of any government scheme from your Gram Panchayat or Tehsildar office before making any payment for getting the subsidy.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.

Don'ts:

- ✕ Never believe in such stories of getting subsidies over calls.
- ✕ The eligible beneficiary data is already available with the State Government.
- ✕ The government will provide you with the benefits after you register yourself at Jan Seva Kendra of your Tehsildar office in your district or gram panchayat.
- ✕ Never share your OTP with anyone.

Don't:

✕ Do not pay money to unknown companies and enrol in unknown schemes.

26. FRAUD USING PUBLIC WI-FI

Do's:

- One should always use a secured Wi-Fi network.
- Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.

27. FAKE ADVERTISEMENTS/OFFERS

Do's:

- ✓ In the case of branded products, verify the advertisements on official websites.
- ✓ For non-branded product advertisements, make a payment only after a personal visit to the shop or on delivery.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.

Don'ts:

- ✕ Don't be misled by tall claims made in advertisements. Check and verify before committing your hard-earned money.
- ✕ Do not pay any amount unless you receive the product.

28. FAKE LOAN OFFER

Do's:

- ✔ Always check the details of the lender (like their physical address/official website, etc.) before availing their loans.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.

Don't:

✕ Never make any upfront payment for sanctioning your loan. Banks and Financial Institutions never ask for advance fee for loan approval. Charges, if any, will be deducted from your loan money and balance amount will be transferred to your account.

30. CREDIT CARD LIMIT UPGRADATION FRAUD

Do's:

- Immediately call the bank to block the card/account/UPI service to prevent further transactions.
- Send an email /letter / visit your home branch to report the incidence.
- Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.

Sometime later, Raju received an SMS from his bank about debit of Rs 70000 on his credit card. He was cheated by the fraudster.

Don'ts:

- ✕ Don't trust unknown callers for credit card activation / limit enhancements.
- ✕ Don't share your card details/OTP with anyone.

32. ONLINE FRAUD USING CASHBACK OFFERS

Raju is very active on the internet and always prefers online shopping as E-commerce websites provide attractive offers on their products.

Dos-

- ✓ Inform your home branch and block your account to prevent further financial loss.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.

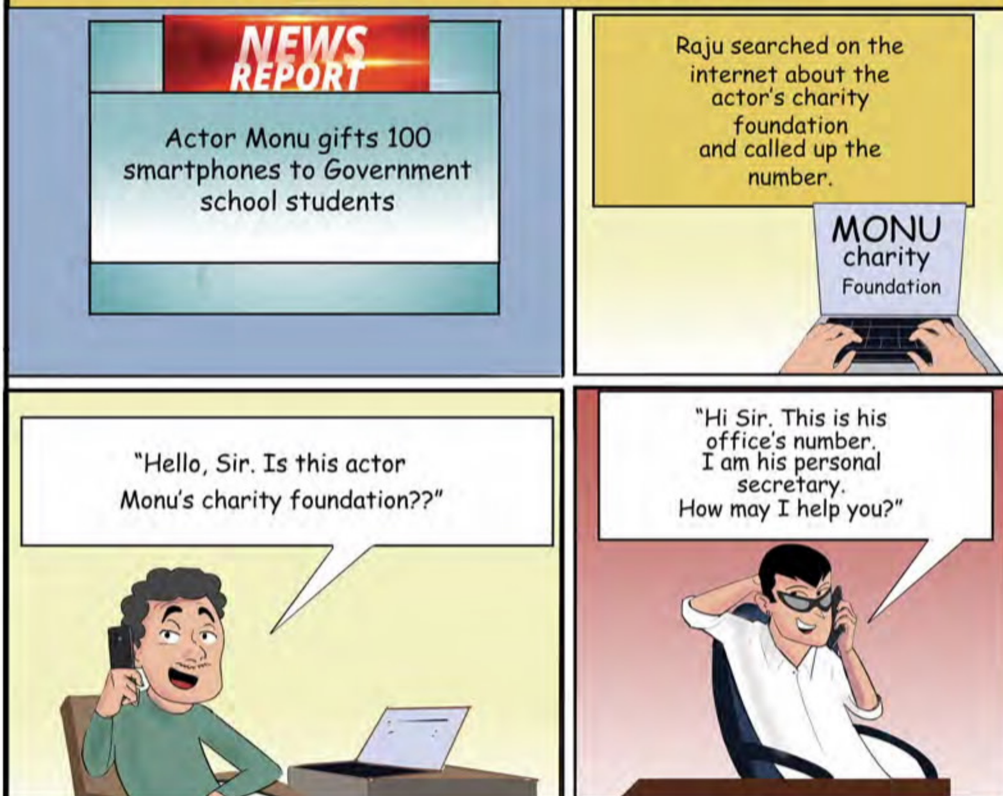
(The moment Raju entered his UPI PIN, an amount of Rs 20,000/- was debited from his account. Raju tried calling the Fraudster but was unable to connect.)

Don'ts-

- × Don't believe the caller blindly; one should verify the company's official website to check the authenticity of the offer.
- × Don't enter or share UPI PIN for receiving payments as it is required only for sending payments.

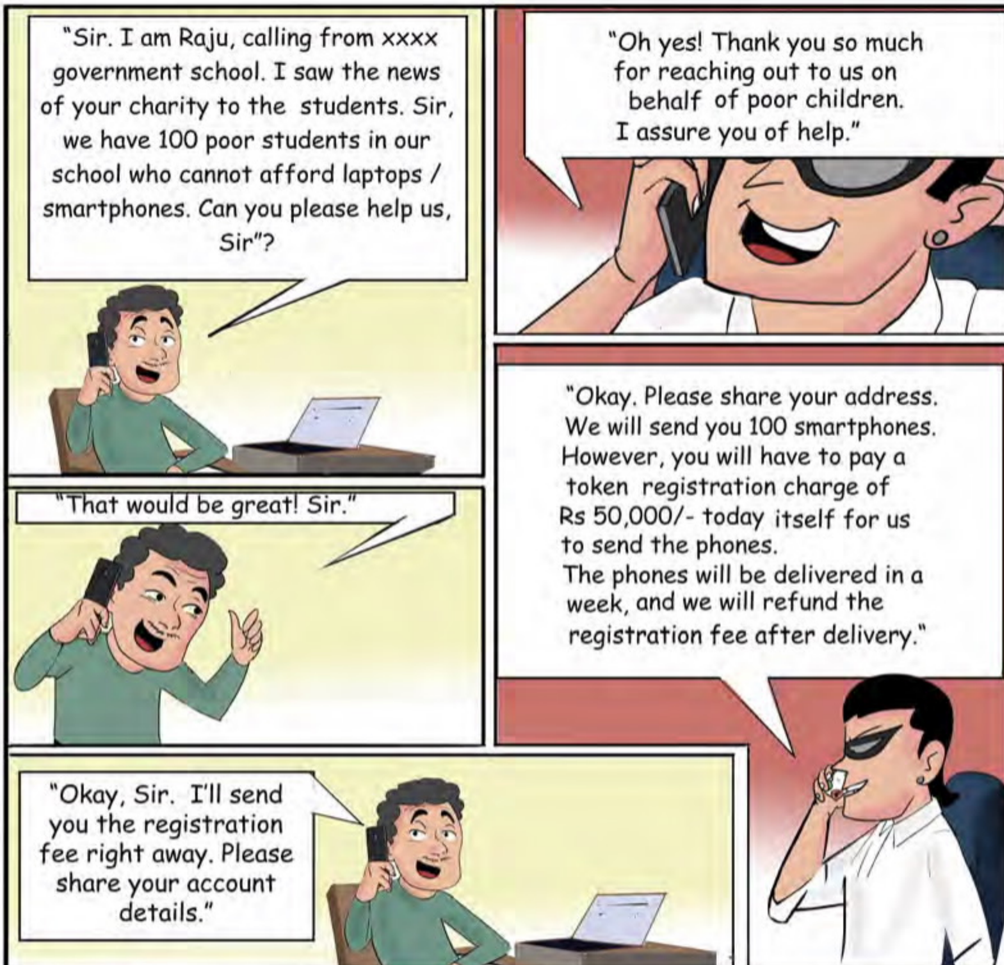
34. CHARITY FRAUDS

Raju is a Government school teacher.
He came across a news report that Actor Monu
was gifting smartphones to government school students.



Do's-

- Always cross-check charity organizations' credentials on the Goverment website /database to see if they are genuine or fake.
- Always be vigilant because the fake website may look almost identical to a genuine charity site, changing only the details of where to send donations.
- Scammers often use high-pressure tactics, such as stressing the urgency and using highly emotive language. Always be cautious of anyone claiming that donations need to be immediate.
- Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in



Raju transferred the funds, but he later came to know that no such mobile phones were donated to government school students. Raju realised that he had been duped by fraudsters under the pretext of charity.

Don'ts-

- ✕ Don't call on a random number based on a google search without verification.
- ✕ Don't send money upfront without verifying the authenticity/genuineness of the claim.

36. FRAUDS USING MALICIOUS APPLICATION

One day, Raju received a message seeking his willingness to do freelance work. As Raju was unemployed, he immediately dialled the number mentioned in the SMS.

After downloading the application, Raju started working. The work seemed genuine; however, he did not know that the fraudster was observing all his activities on his laptop.

Over time, the fraudster was able to get all the secure credentials from Raju's device through his application. Unaware of the malafide intention, Raju continues to use the application. The fraudster was also able to get the OTP sent on Raju's email since the fraudster got access to his email.

Do's:

- ✓ Verify the authenticity of the offer on the official website of the concerned entity offering jobs.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in."

After a few days, Raju received SMS alerts stating Rs 50,000 was debited from his account Raju had no clue how his account was compromised or money was debited.

After investigation, it was found that his device contained a malicious application, observing all his activities and the passwords were being skimmed.

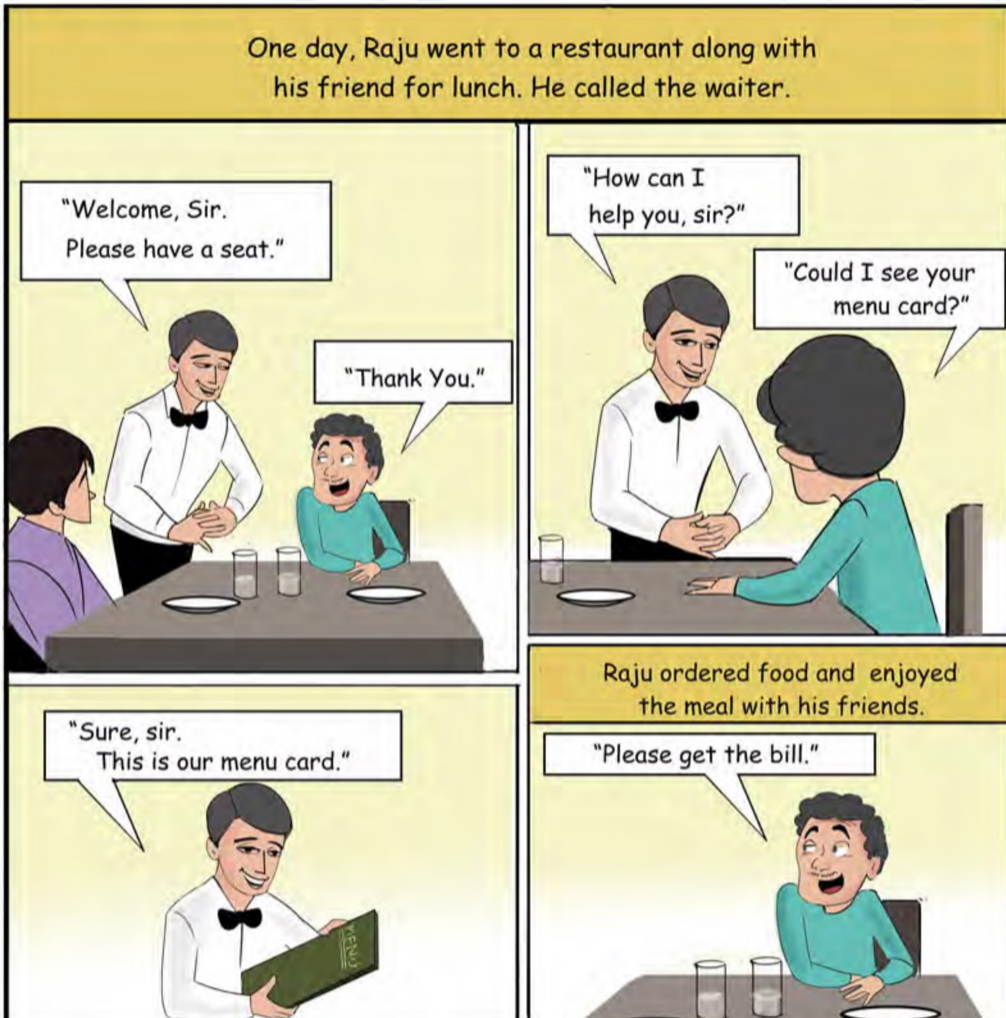
Don'ts:

✕ Do not download any application through links sent via SMS, email or instant messaging applications, especially from strangers, without verifying its authenticity.

Don'ts:

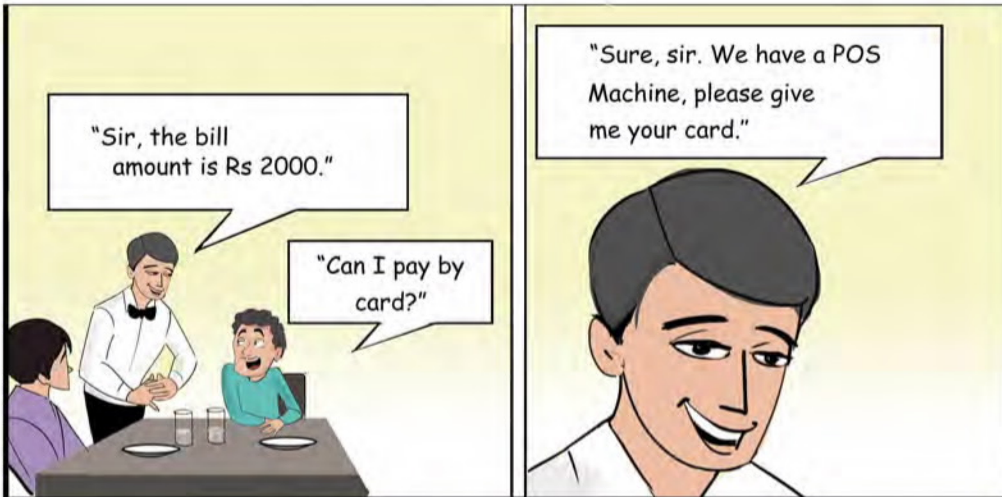
× Be cautious and don't take loan if any mobile app is providing a quick loan without checking any document and credit score, and always check the interest rate charged.

38. CARD CLONING AT MERCHANT OUTLETS

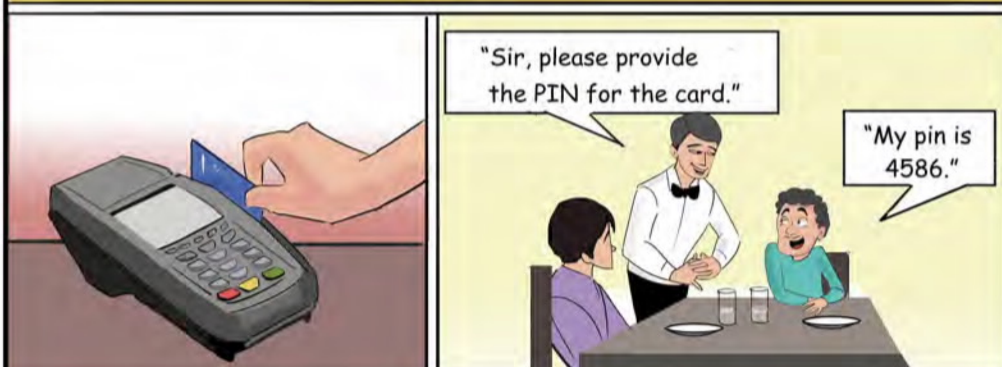


Do's:

- ✔ Always hide your pin number while transacting through debit/credit card.
- ✔ Change the PIN at periodic intervals.
- ✔ Always ask merchants/dealers to swipe the card in your presence.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in."



(Waiter took the card, walked away from Raju and swiped the card in a skimmer when Raju was not paying attention.)



Later, the skimmed details of the card were given to a fraudster who cloned the card with all the card details and used those details to siphon off money from Raju's account.

Don't:

✕ Do not share your credit card/Debit card PIN with anyone.

✕ Do not let credit and debit cards out of your sight.

Office of the RBI Ombudsman (Mumbai-II)
Maharashtra And Goa

Design, content & execution: Raj Kumar, M Muralidhar, Forum Modi, Vishwas Krishna, P P Bhagat

Cover Design, Layout & Illustration by **StoryMirror**