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!

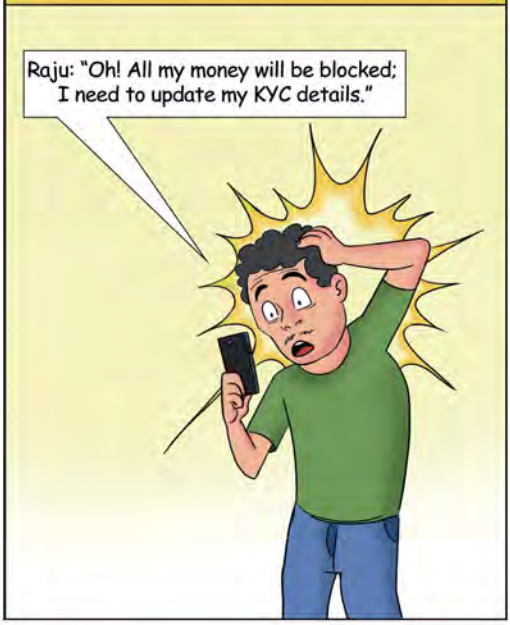
INDEX

SL. No.	Topic Name	Page Number
1	FRAUD THROUGH PHISHING LINKS	1
2	VISHING CALLS	3
3	FRAUD USING ONLINE MARKETPLACES	5
4	CREDIT CARD ANNUAL FEE WAIVER- FAKE OFFER	7
5	ATM CARD SKIMMING FRAUD	9
6	FRAUD USING SCREEN SHARING APP/REMOTE ACCESS	11
7	SIM SWAP/ SIM CLONING	13
8	FRAUDS BY COMPROMISING CREDENTIALS THROUGH SEARCH ENGINES	15
9	SCAM THROUGH QR CODE SCAN	17
10	IMPERSONATION THROUGH SOCIAL MEDIA	19
11	JUICE JACKING – STEALING OF DATA THROUGH CHARGING CABLE	21
12	LOTTERY FRAUD	23
13	ONLINE JOB FRAUD	25
14	FAKE ACCOUNT NUMBER	27
15	FRAUD THROUGH EMAIL	29
16	MESSAGE APP BANKING FRAUD	31
17	FRAUDULENT LOANS WITH STOLEN DOCUMENTS	33
18	BETTING SCAM	35
19	FAKE VACCINATION CALL	37
20	COVID TESTING- FAKE ONLINE SITE	39

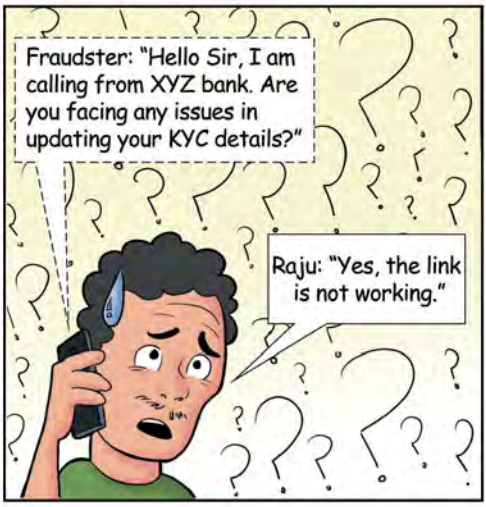
SL. No.	Topic Name	Page Number
21	FRAUDSTERS IN THE PRETEXT OF RECOVERY AGENTS	41
22	SOCIAL WELFARE SCHEME FRAUD	43
23	MULTI-LEVEL MARKETING (MLM) SCAMS	45
24	WORK FROM HOME SCAM	47
25	ONLINE SHOPPING FRAUD	49
26	FRAUD USING PUBLIC WI-FI	51
27	FAKE ADVERTISEMENTS/OFFERS	53
28	FAKE LOAN OFFER	55
29	CREDIT CARD ACTIVATION FRAUD	57
30	CREDIT CARD LIMIT UPGRADATION FRAUD	59
31	SAFE GUARDING YOUR AADHAAR CARD	61
32	ONLINE FRAUD USING CASHBACK OFFERS	63
33	DISCOUNT FRAUD	65
34	CHARITY FRAUDS	67
35	OVERDRAFT AGAINST FD	69
36	FRAUDS USING MALICIOUS APPLICATION	71
37	ILLEGAL LOAN FINANCING APPS WITH EXORBITANT INTEREST RATES AND HARASSMENT TACTICS	73
38	CARD CLONING AT MERCHANT OUTLETS	75
39	FRAUD THROUGH DETAILS SHARED WITH KNOWN PERSON/FAMILY/RELATIVES	77
40	PAYMENT SPOOFING APPLICATIONS.	79

1. FRAUD THROUGH PHISHING LINKS

One day, Raju received message on his phone: *'Dear customer, if your KYC details are not updated within two days, your account will be blocked. Use the below link to update the details at http://updateKYC.XYZbank.com'*

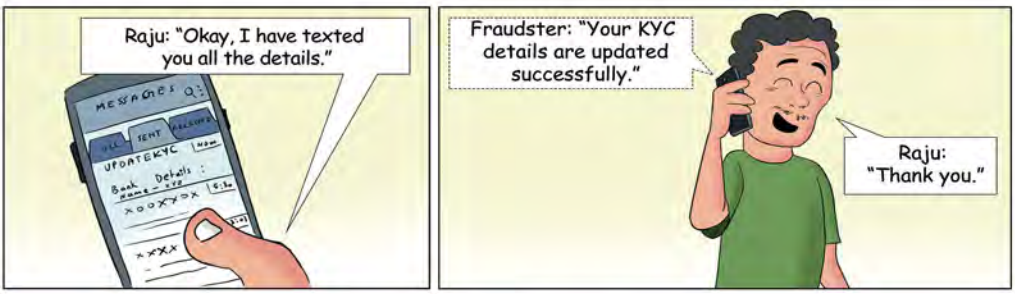


Raju clicked on the link, but the link to update KYC details did not work. Soon, he gets a call.



Do's:

- ✓ Always cross-check the KYC status with your home branch or through your relationship manager when you receive calls, links or SMS from unknown sources requesting you to update KYC.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in



After some time, Raju received SMS alerts on his phone stating that Rs 50,000 was debited from his account.

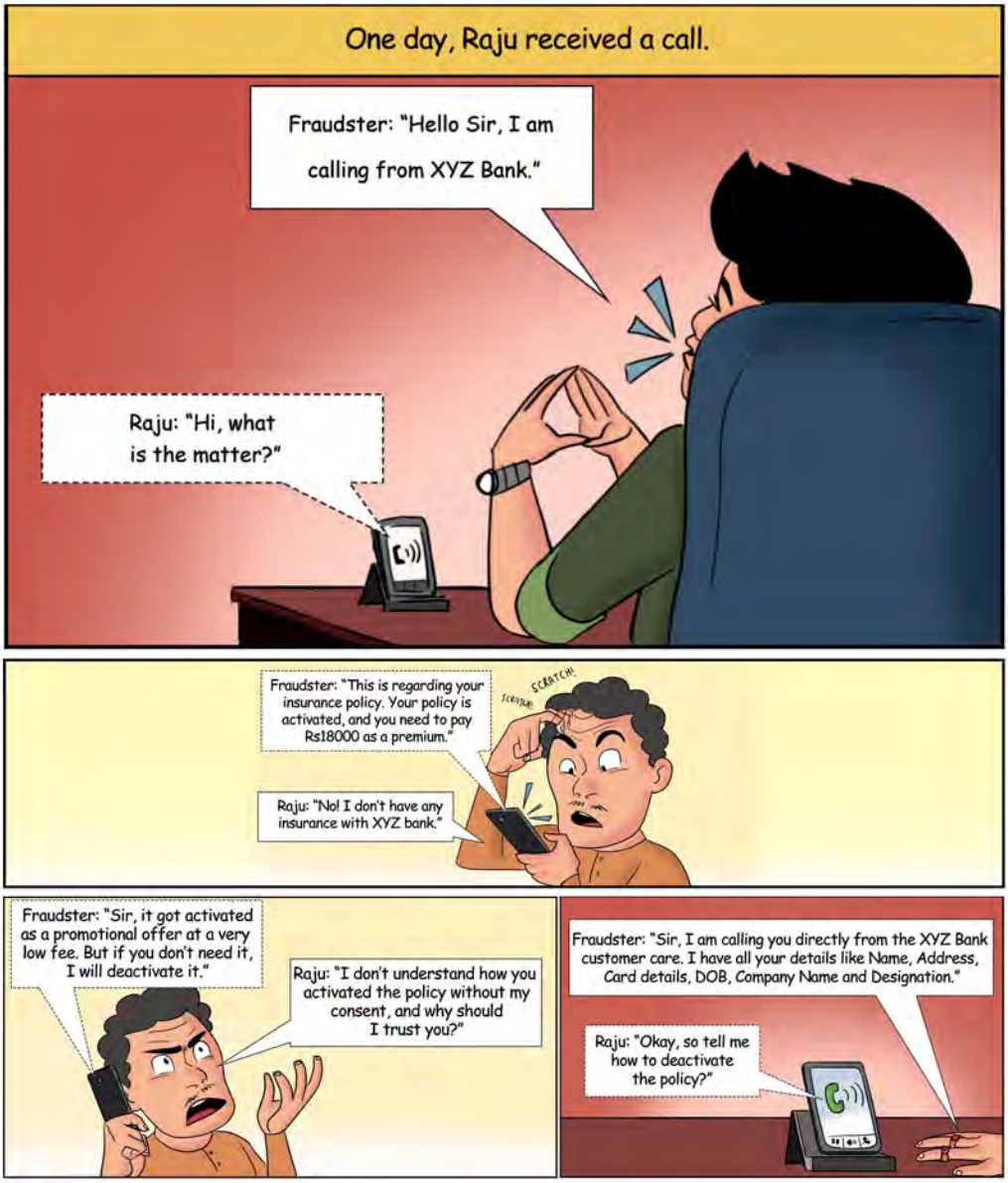
Raju immediately called the other person, but he didn't answer the calls. Raju realized that the person was a fraudster and he should not have shared any personal details with him.

Don'ts:

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

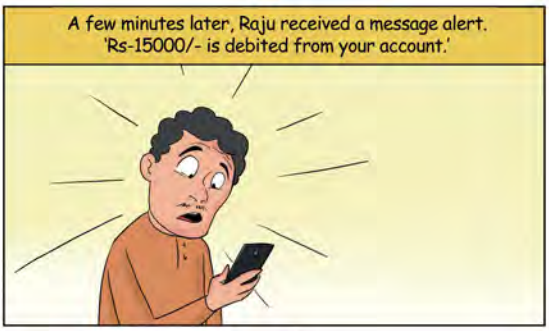
× Don't share your confidential details with strangers.

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

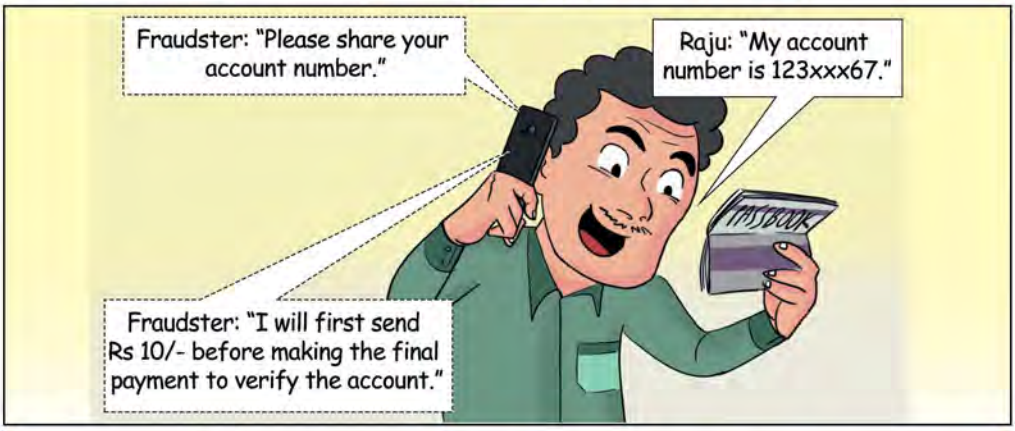


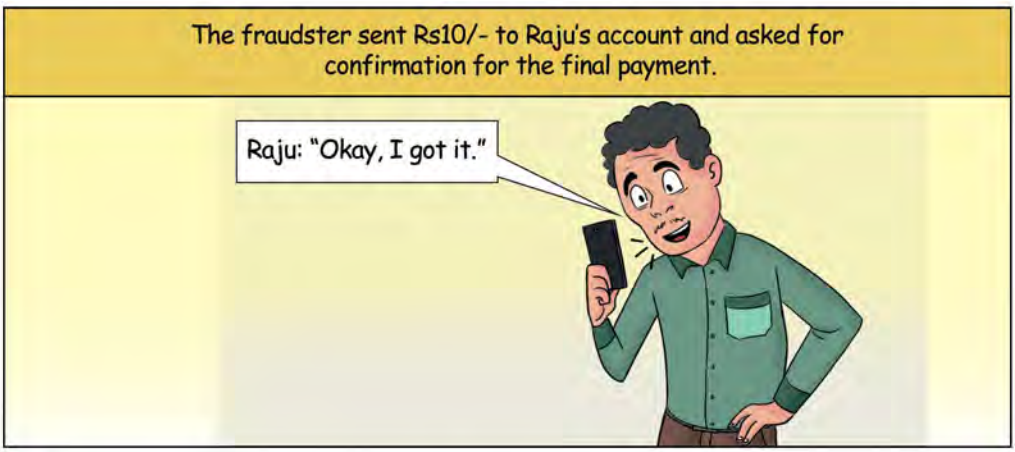
Raju immediately visited the nearby XYZ branch and enquired about the transaction.
Raju realized his mistake: the call was from a fraudster;
he should not have believed a stranger.

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





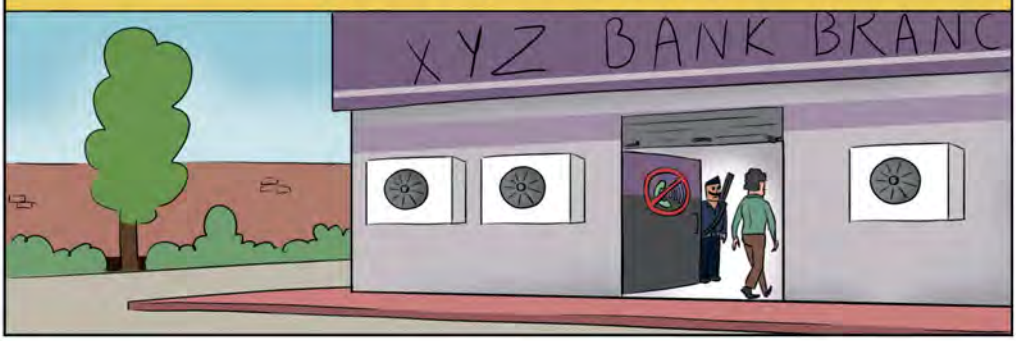
Do's:

- ✓ **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**

Then the fraudster sent a UPI request for receiving a payment of Rs 14,990/- instead of paying Raju.

Raju entered the pin immediately, and his account was debited for Rs14,990/-

Realizing that he was cheated, Raju quickly approaches the bank branch and registered a complaint on the same day.

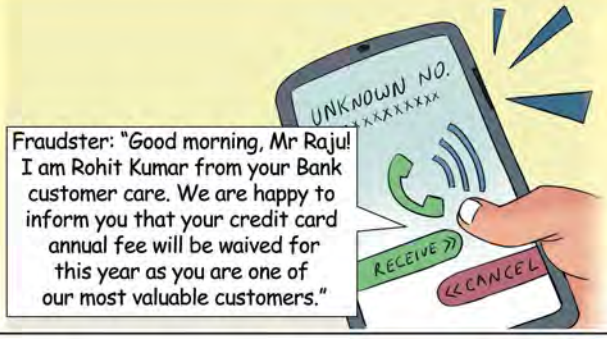


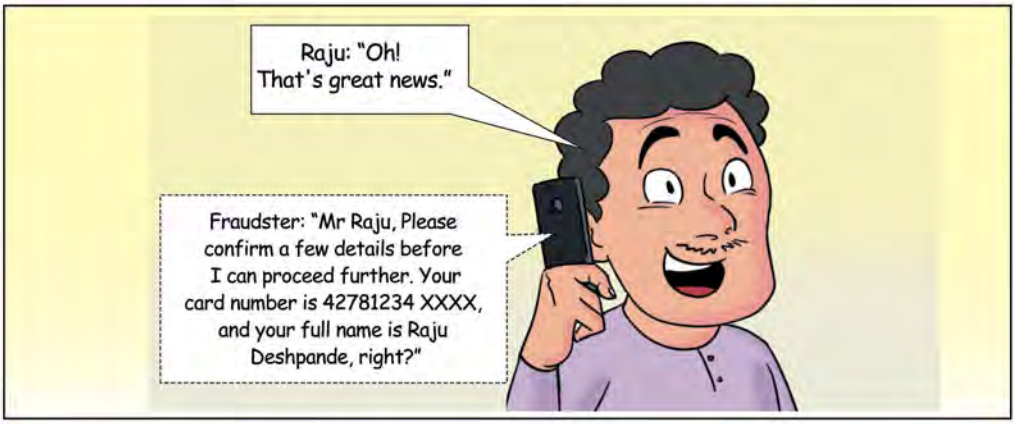
Don'ts:

- × **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

One day, Raju received a call from an unknown number.





The fraudster had already gathered Raju's card details from illegitimate sources.

Do's:

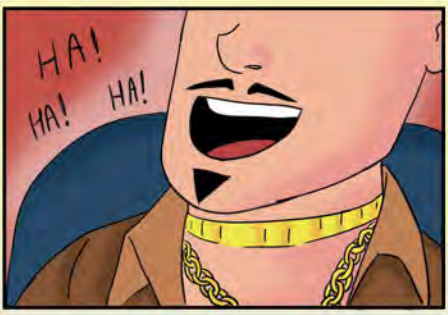
- ✓ Be cautious while responding to calls from unknown numbers claiming to be from your bank.
- ✓ Report to your Homebranch immediately on realizing the fraud.
- ✓ Block your card to prevent further financial loss.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime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

Raju reasoned that since the caller already knew his card details, the call must be genuine. He shared the OTP with the fraudster immediately.

The call was disconnected. Soon, Raju received an SMS stating that Rs12,000 was debited from his credit card account.

Raju immediately called the fraudster, but his phone was switched off.

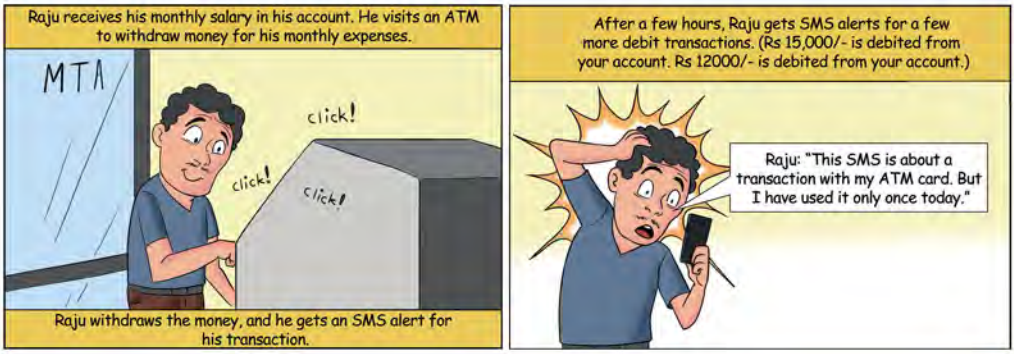
Raju realized the person was a fraudster, and he should not have shared the OTP with him.

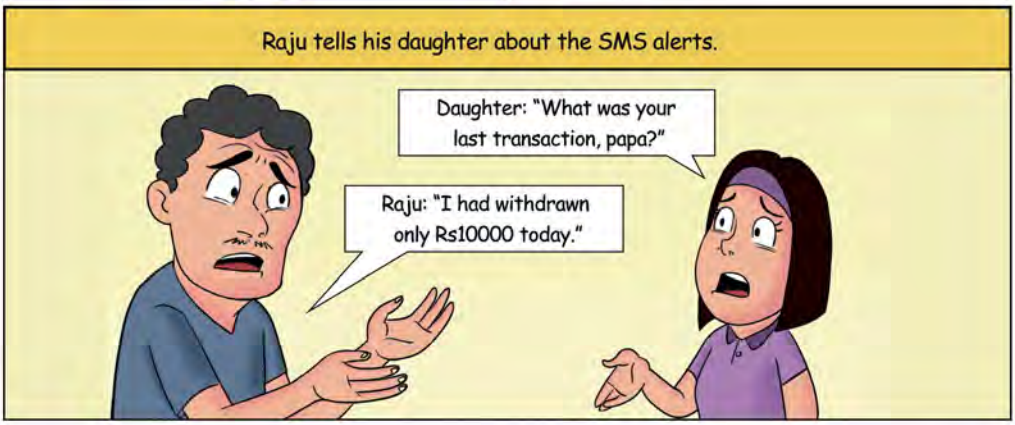


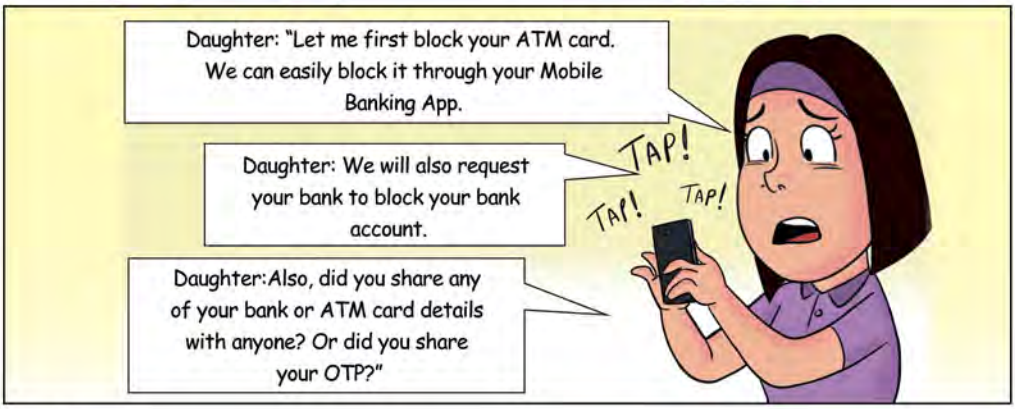
Don'ts:

× **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

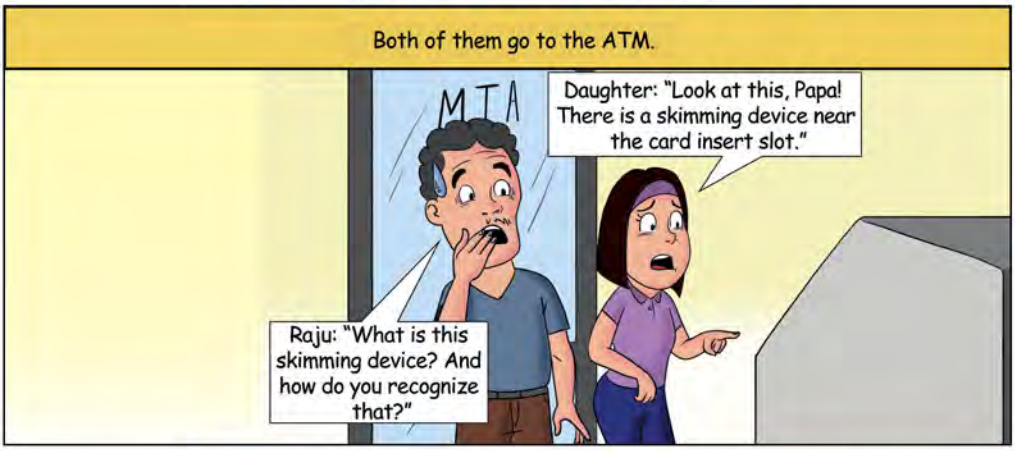






Do's:

- ✔ 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:

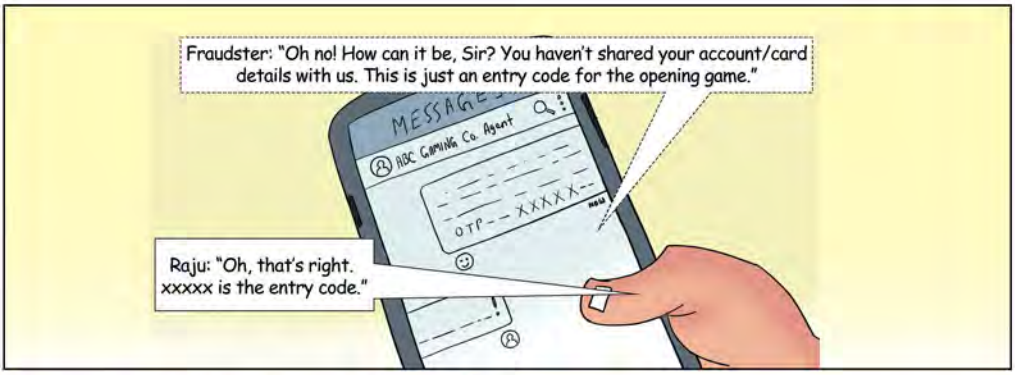
× Don't give your ATM card to anyone on the ATM premises to transact on your behalf. This kind of social engineering is being used to target senior citizens/semi-educated persons who have difficulty operating ATMs.

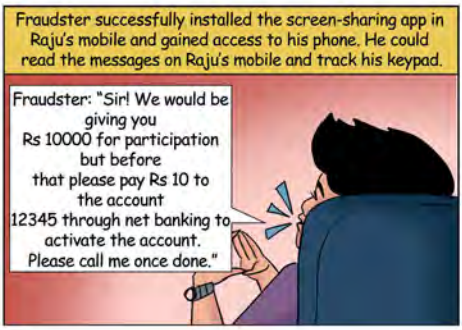
6. FRAUD USING SCREEN SHARING APP/REMOTE ACCESS

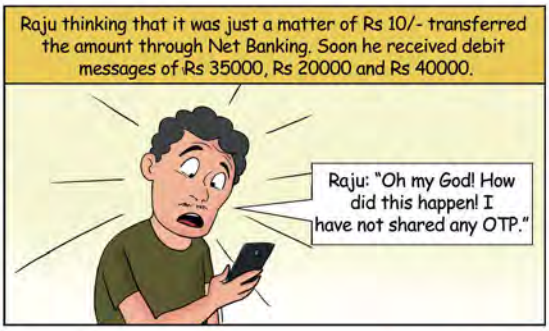
At first, Raju doubted that the person might be a fraudster and remained silent.

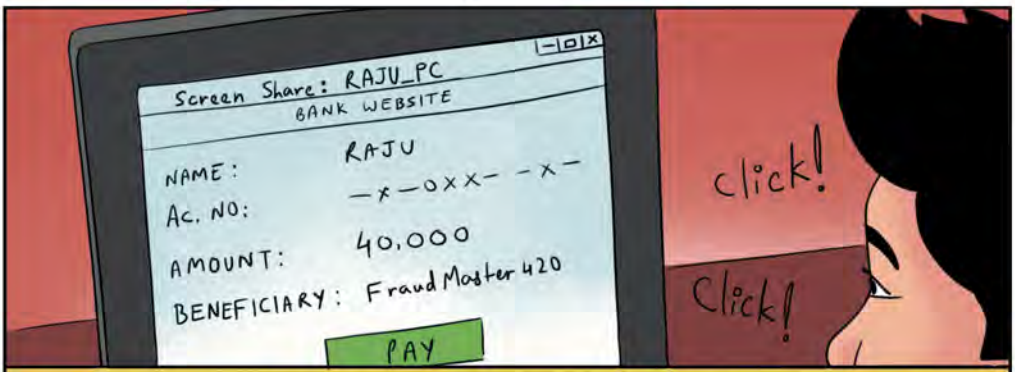
Do's:

- ✔ 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









Once the screen-sharing application was installed, the fraudster had access to the net banking password entered by Raju for making the payment (of Rs 10.)

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

Raju shares the details with the caller.

Fraudster uses the new SIM to retrieve the username for the banking application by using options like forgot username, reset password etc. and transfer all the money to his account.

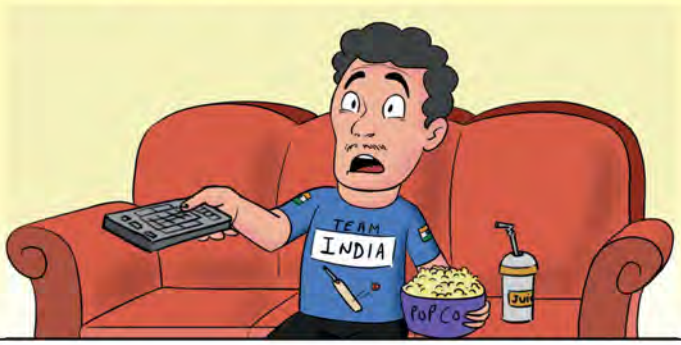
After a few minutes, when Raju received emails showing cash debits from his bank account, he checked his bank account balance. He noticed that some unauthorized debits were made from his account for which no SMSs were received on his registered mobile number as the SIM was compromised to transfer funds, shop online, etc.

Don'ts:

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

8. FRAUDS BY COMPROMISING CREDENTIALS THROUGH SEARCH ENGINES

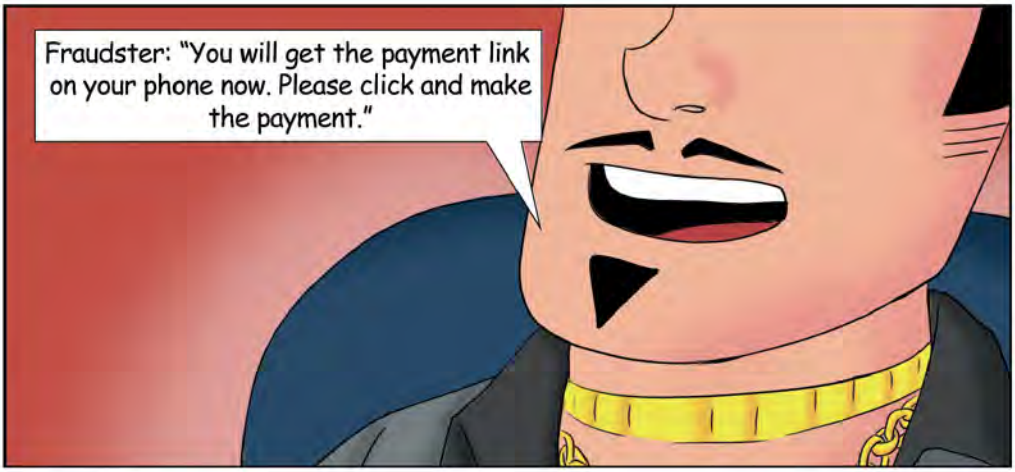
Raju is fond of watching cricket, and he was very excited about the upcoming cricket match. But as soon as he opened the Sports App, he realised that his subscription had expired.

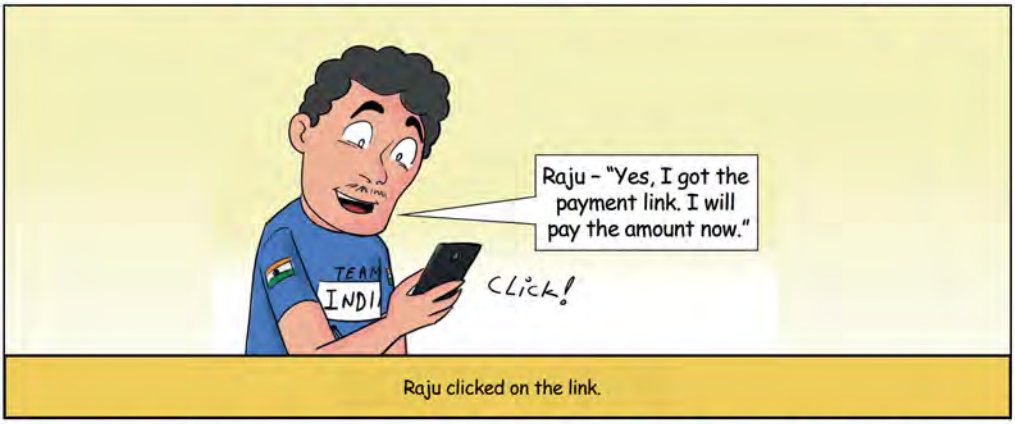


Thinking this, he searched for a way to recharge the Sports App on the internet. After searching for a while, he found a phone number for the same. Raju dialled the number immediately.

Do's:

- ✓ Always obtain the contact details/customer service number, etc. from the official website of the service provider only.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in





Raju clicked on the link.

Raju received an SMS stating that Rs 40,000 was debited from his account.

Instead of paying Rs 1000 to Sports App, Raju ended up transferring Rs 40000 to the fraudster.

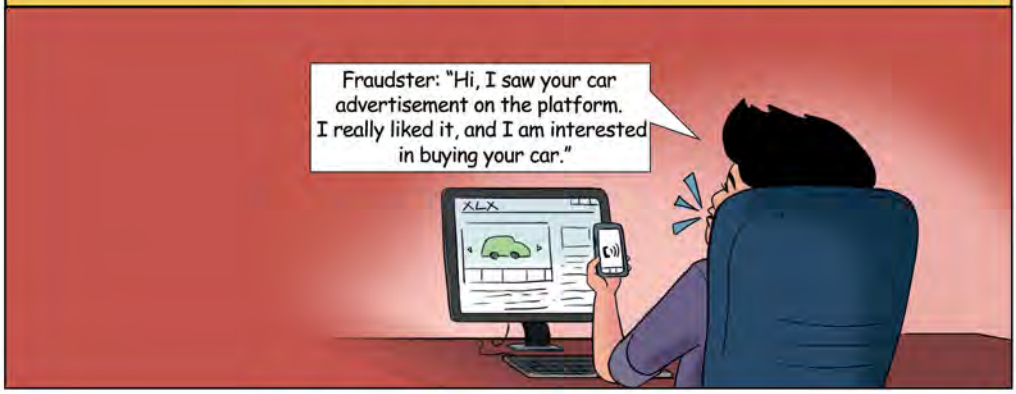
Don'ts:

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

9. SCAM THROUGH QR CODE SCAN

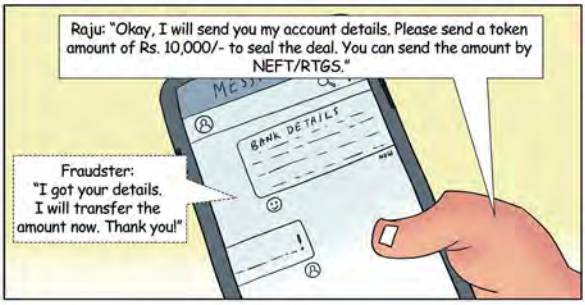
Raju registered his old car on an online website to sell it.

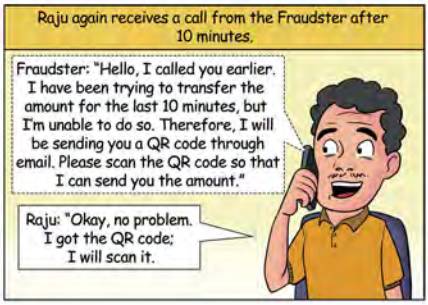
Within hours, he was contacted by a person (a fraudster)

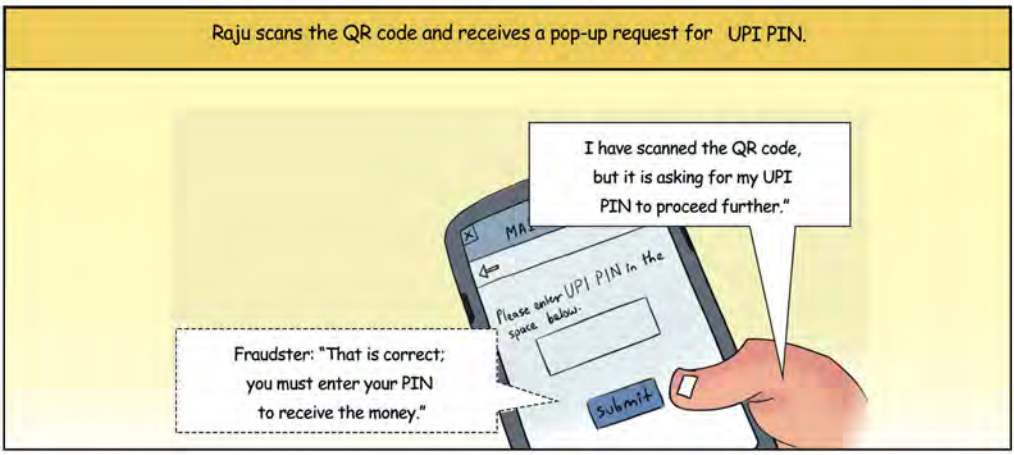


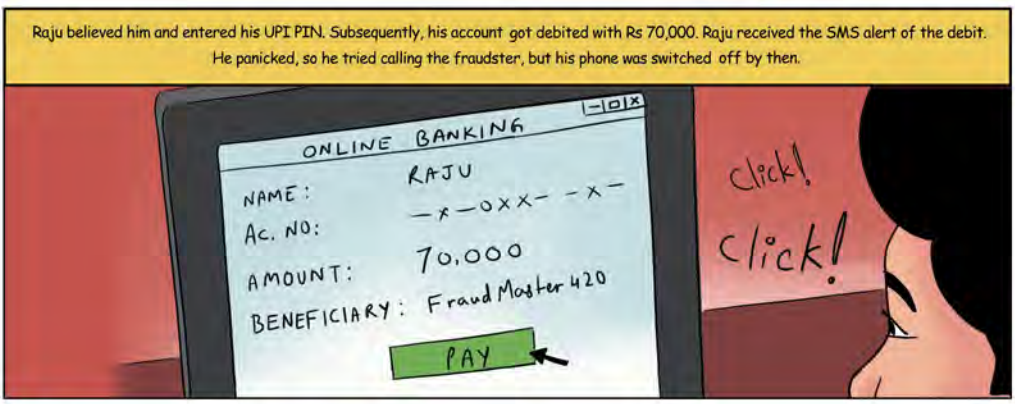
Do's:

- ✓ 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





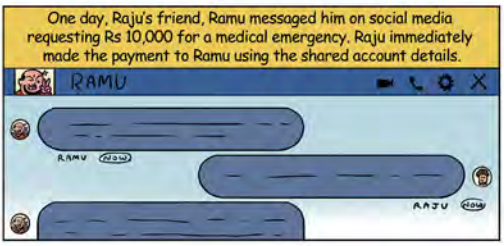




Don'ts:

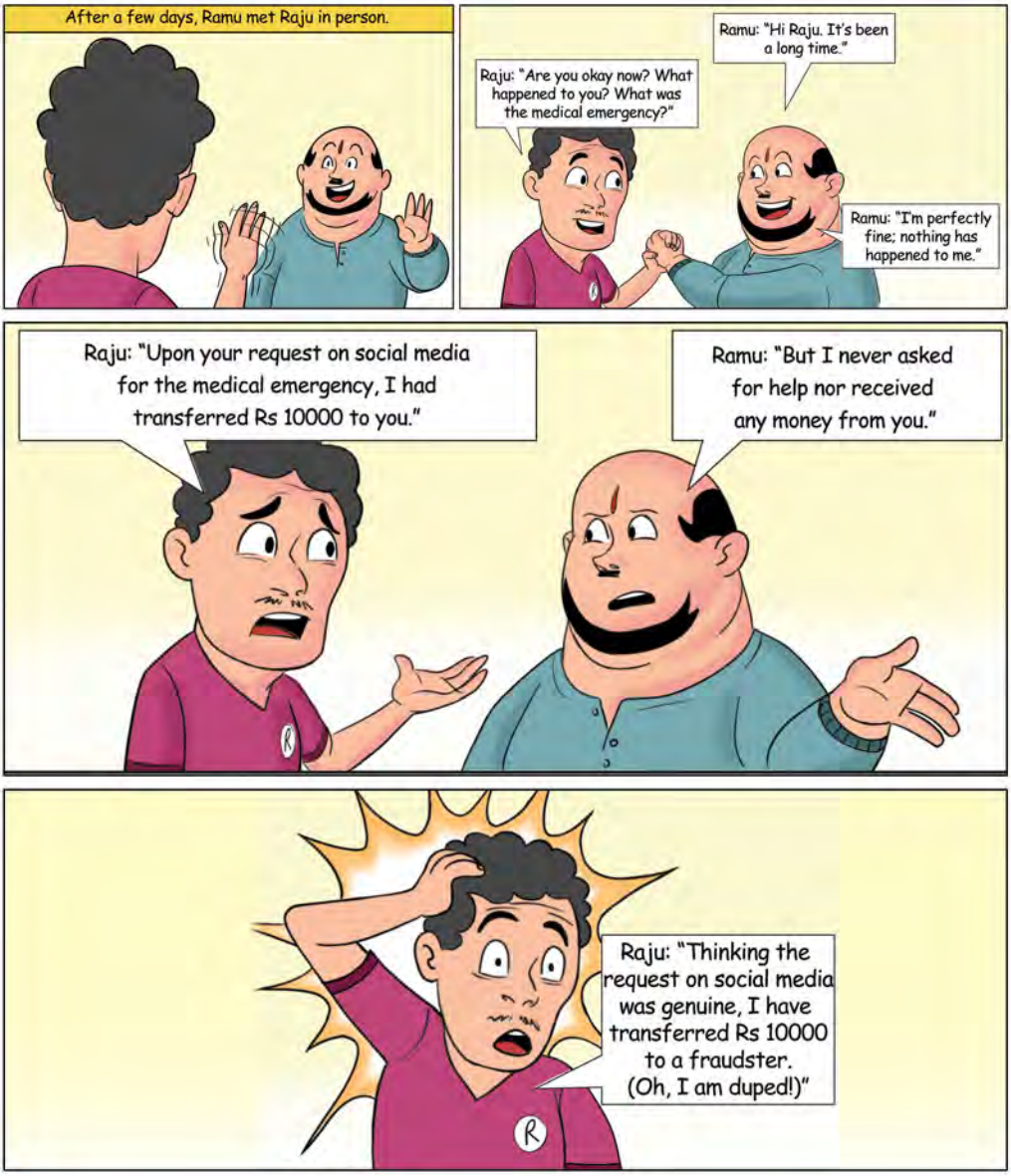
- × Don't enter your UPI PIN to receive money from another person. UPI PIN is required only for sending a payment, not for receiving.
- × Don't scan QR codes to receive any payment. QR code needs to be scanned for sending a payment, not for receiving Money.

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



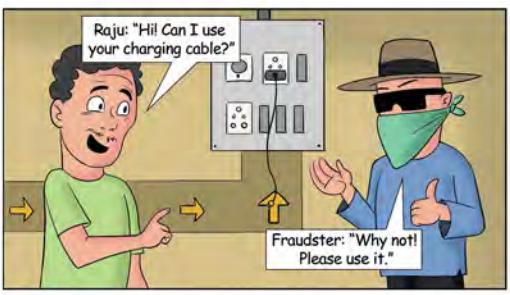
Don'ts:

- × 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

Raju had to leave due to a medical emergency.
He realizes that his phone battery is low.

A fraudster installs a charging cable with a virus and leaves it at the charging point in a public place. Raju notices the charging point with the charging cable and asks the fraudster if he can use it.



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

While charging, the charging cable injects the virus into Raju's mobile.

During the next few days, the fraudster captured all details entered by Raju on his mobile and got hold of vital bank details like username, password etc.

One day, Raju receives SMSs/emails indicating unauthorized debits in his savings account...

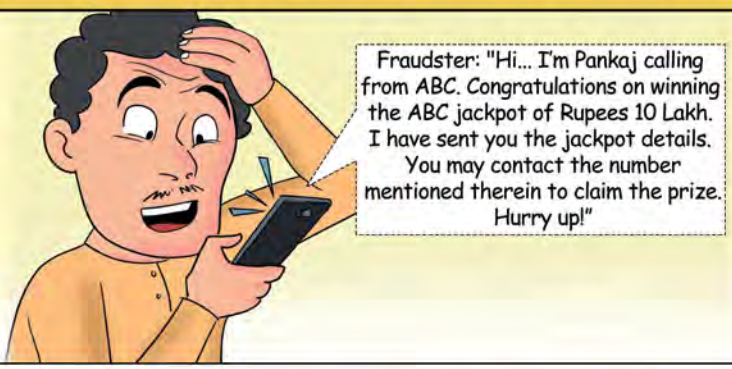
...and realizes that his account has been compromised somewhere.

Don'ts:

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

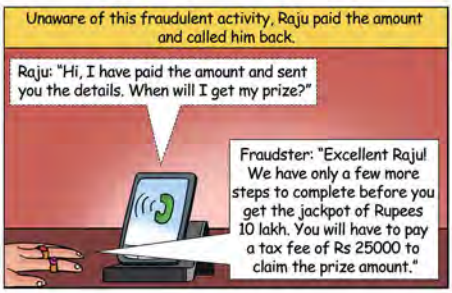
12. LOTTERY FRAUD

Raju received an audio message stating that he had won an ABC jackpot.



Excited, Raju called the number in the jackpot message which featured a fake audio of a Superstar congratulating him on the prize. He contacted the given number.

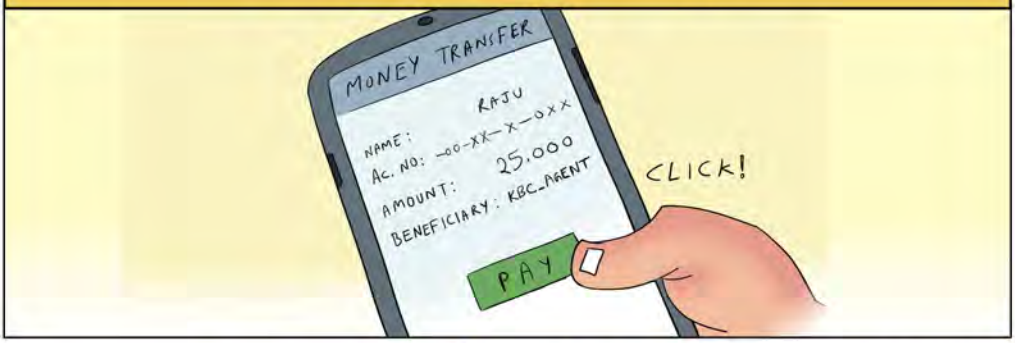
Unaware of this fraudulent activity, Raju paid the amount and called him back.



Do's:

- ✓ Verify the message received from unknown numbers before trusting them as members of any company or management team.
- ✓ Always verify lottery offers with official websites of such events.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in

Without thinking twice, Raju makes the payment.



Raju waits for the jackpot for the next few days but receives no further updates...

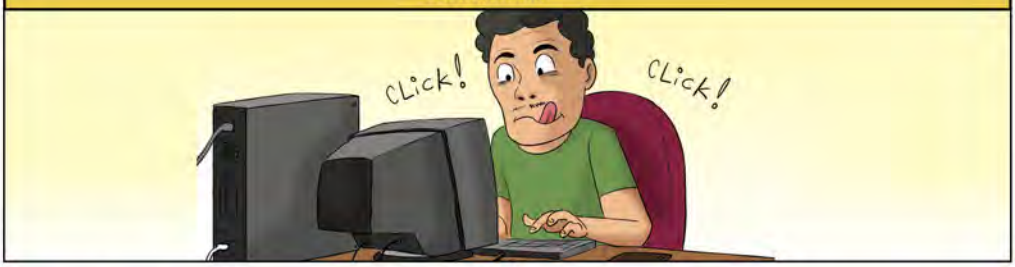
...Later, he realizes that he was cheated.

Don'ts:

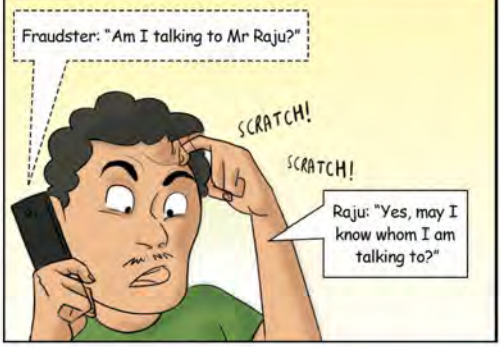
× Do not make payments without verification, expecting very high returns.

13. ONLINE JOB FRAUD

Raju had lost his job recently and was very worried. He started looking for jobs on online job portals. He updated his resume on various websites.



One day, he got a call from a fraudster, impersonating a person from XYZ Company.



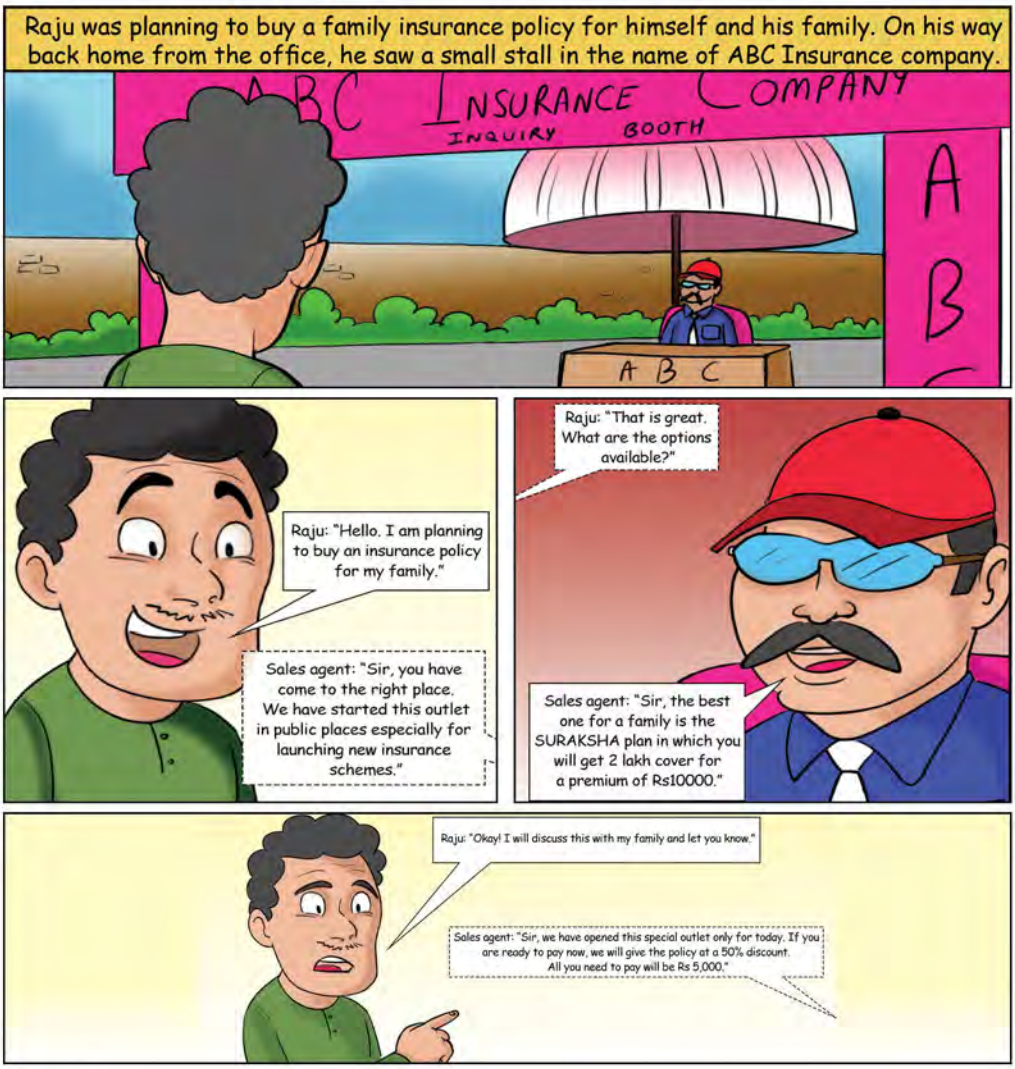
Do's:

- ✓ 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:

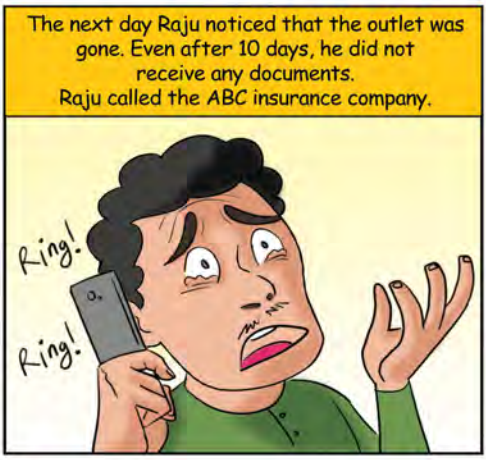
✕ Don't pay anyone under the pretext of a job. A legitimate company will never ask for payment from a potential candidate for a job offer.

14. FAKE ACCOUNT NUMBER



Do's

- ✓ Cross-check an organization's credentials on a known database to see if they are genuine.
- ✓ Always approach registered offices for availing products.
- ✓ Funds are transferred solely based on account number.
- ✓ Fraudsters may give a genuine company name but give their own account number, always verify the account number with the company before making a payment.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in



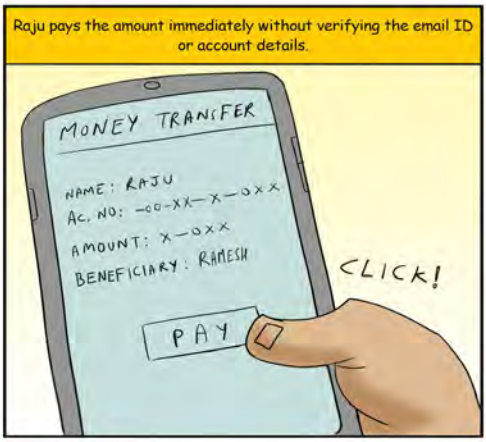
Don'ts:

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

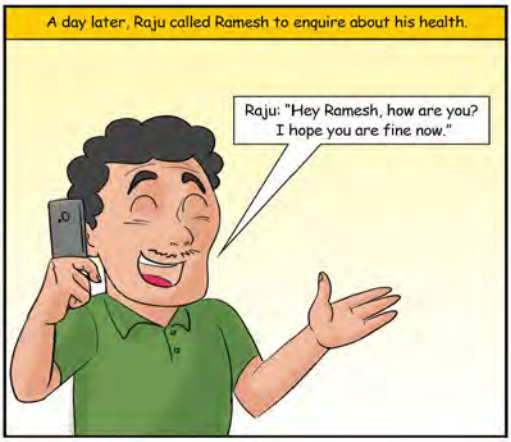
15. FRAUD THROUGH EMAIL

A fraudster sent an email to Raju, impersonating his friend Ramesh, asking for financial help for his medical emergency.

Raju pays the amount immediately without verifying the email ID or account details.



A day later, Raju called Ramesh to enquire about his health.



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.

16. MESSAGE APP BANKING FRAUD

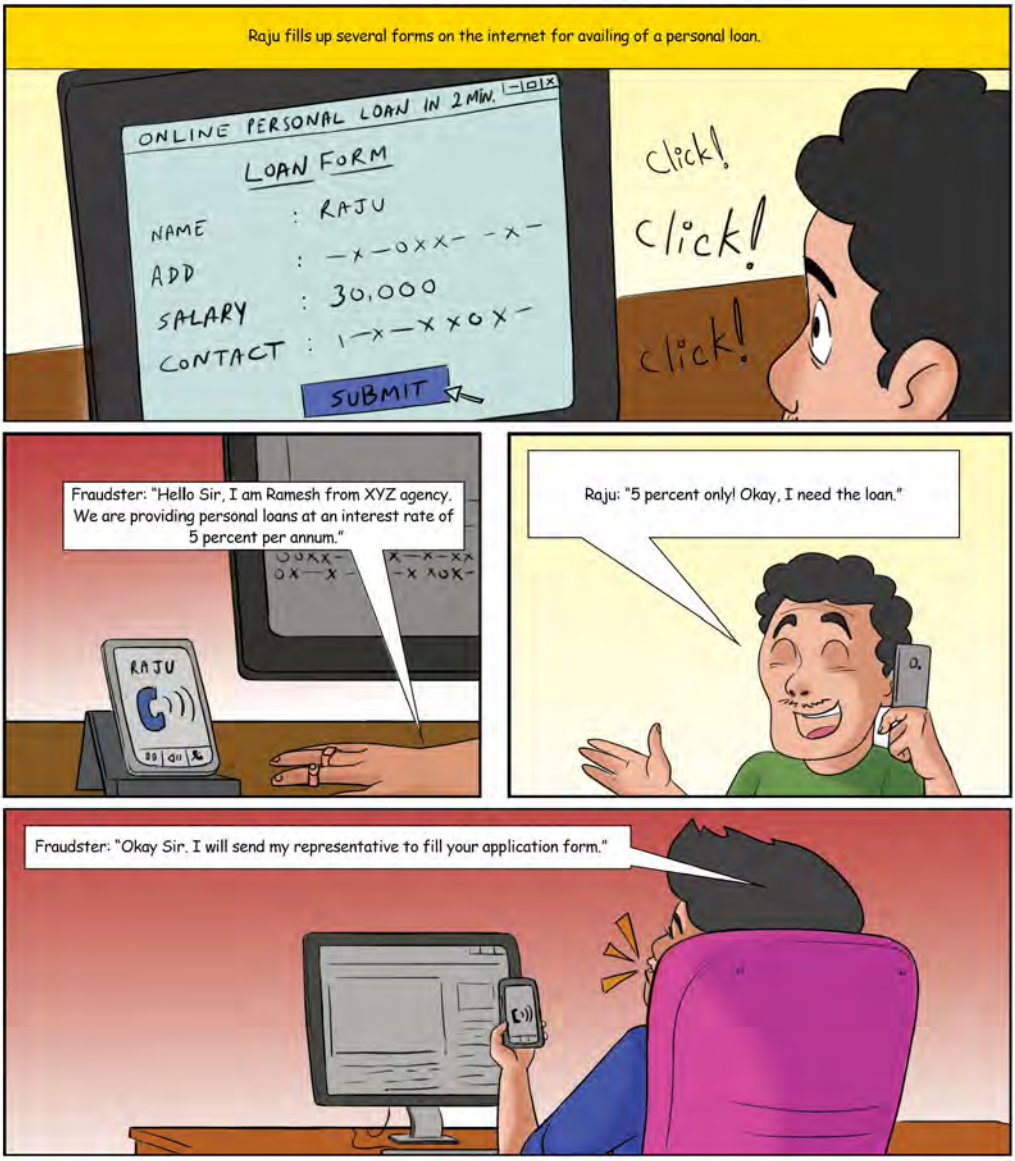
Do's:

- ✔ Be cautious while responding to calls from unknown numbers seeking your account details.
- ✔ Report to your home branch immediately on realizing the fraud. 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.

Don'ts:

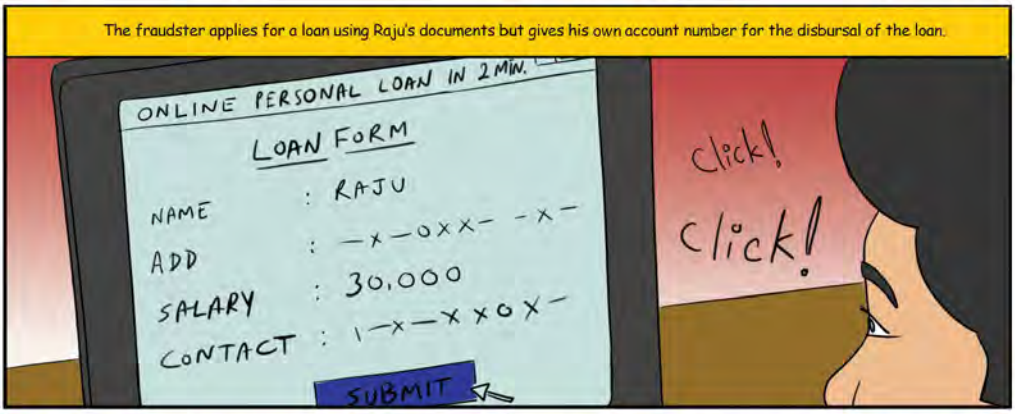
- ✕ Don't trust unknown callers offering easy banking services and sending texts through Messaging Apps.
- ✕ Don't share card details and OTP.

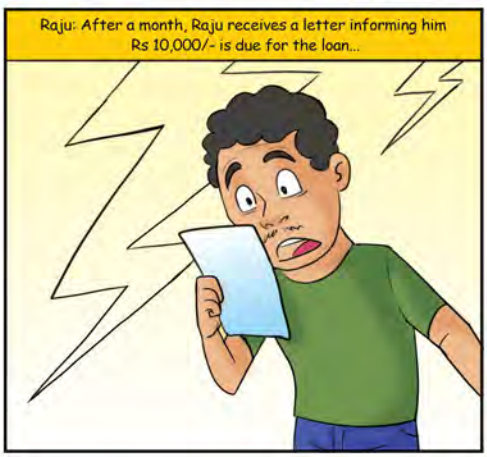
17. FRAUDULENT LOANS WITH STOLEN DOCUMENTS



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





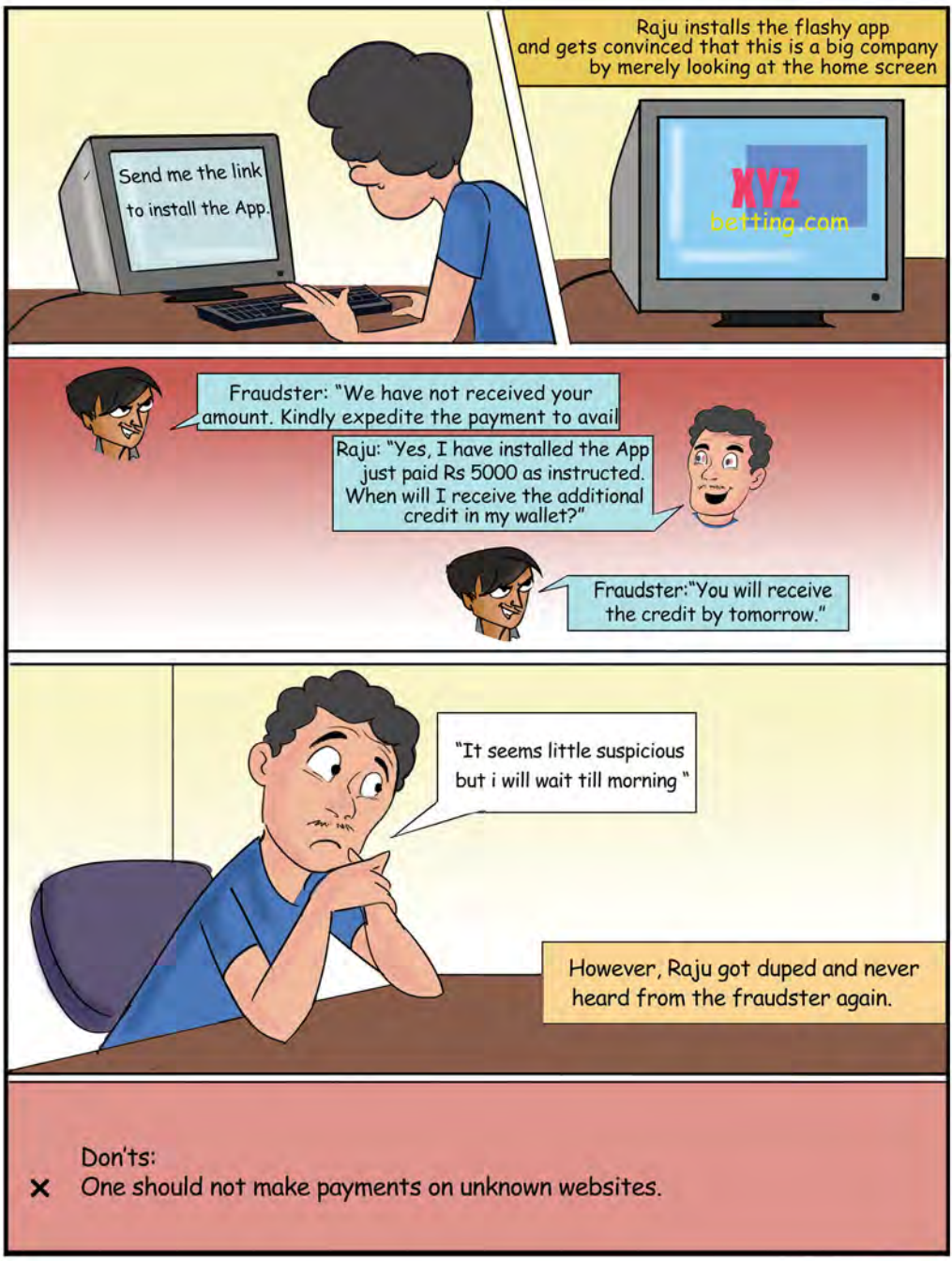
Don'ts:

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

18. BETTING SCAM

Do's:

- ✔ In case scammed by a fake app/website, one should immediately call his/her bank to block the card/account/UPI service to prevent further transactions.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in


Send me the link to install the App.
Raju installs the flashy app and gets convinced that this is a big company by merely looking at the home screen
XYZ
betting.com
Fraudster: "We have not received your amount. Kindly expedite the payment to avail
Raju: "Yes, I have installed the App just paid Rs 5000 as instructed. When will I receive the additional credit in my wallet?"
Fraudster:"You will receive the credit by tomorrow."
"It seems little suspicious but i will wait till morning "
However, Raju got duped and never heard from the fraudster again.
Don'ts:
× One should not make payments on unknown websites.

19. FAKE VACCINATION CALL

One day, Raju received a call from an unknown number.

Do's:

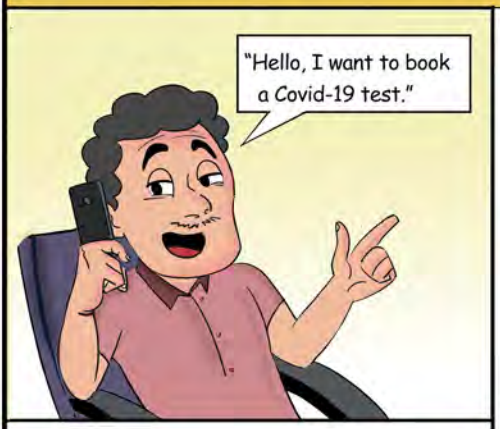
- ✓ Read the entire SMS to read the purpose of OTP.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.

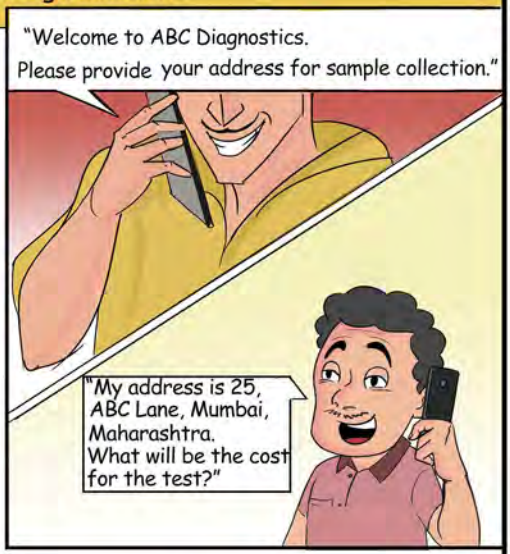
Don'ts:

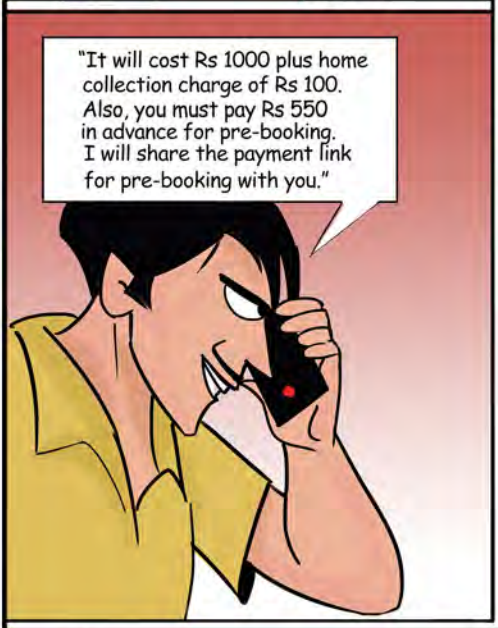
× Don't share your Aadhaar, PAN card details and OTP with strangers.
PAN card-based OTP is used for various financial services including cash withdrawal from bank accounts. Therefore, it is extremely important to protect your confidential details like Aadhar and PAN cards from fraudsters.

20. COVID TESTING- FAKE ONLINE SITE

Raju wanted to do the Covid-19 test at home. He searched on the internet for diagnostic centres that provide home testing facilities.







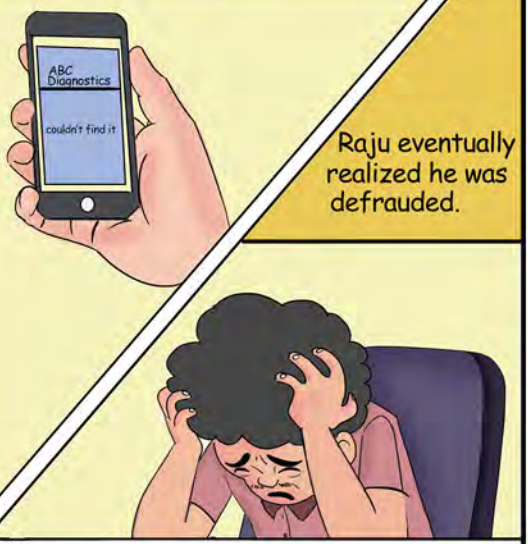
As it was urgent for Raju to get tested, he agreed to pay the advance amount.He paid the said amount using his debit card on the link provided.

Do's:

- ✓ Always book any kind of test through registered pathology laboratories only.
- ✓ 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.

Raju got tensed, and he searched the helpline number on the ABC Diagnostics site but couldn't find it.

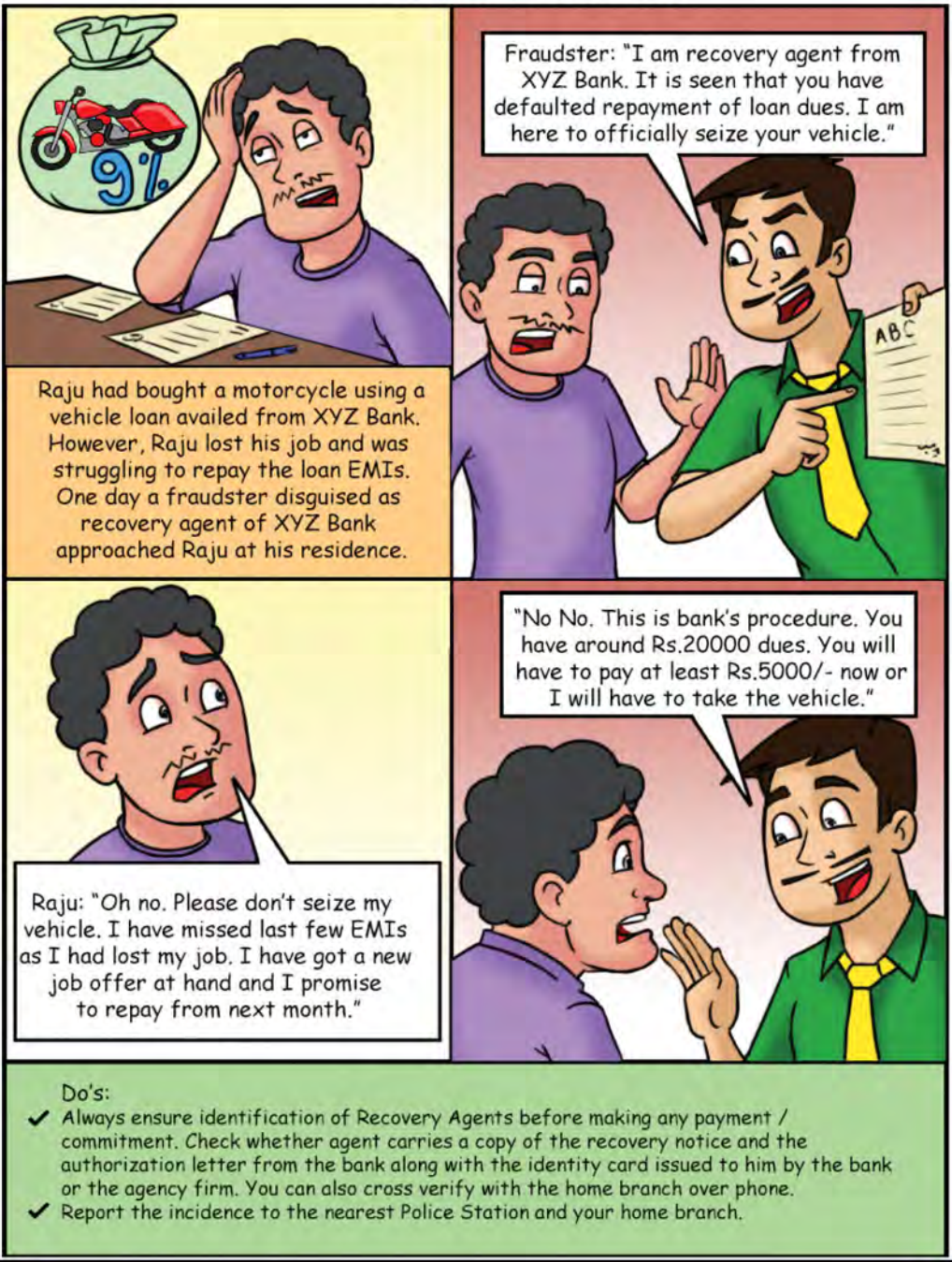


Raju eventually realized he was defrauded.

Don'ts:

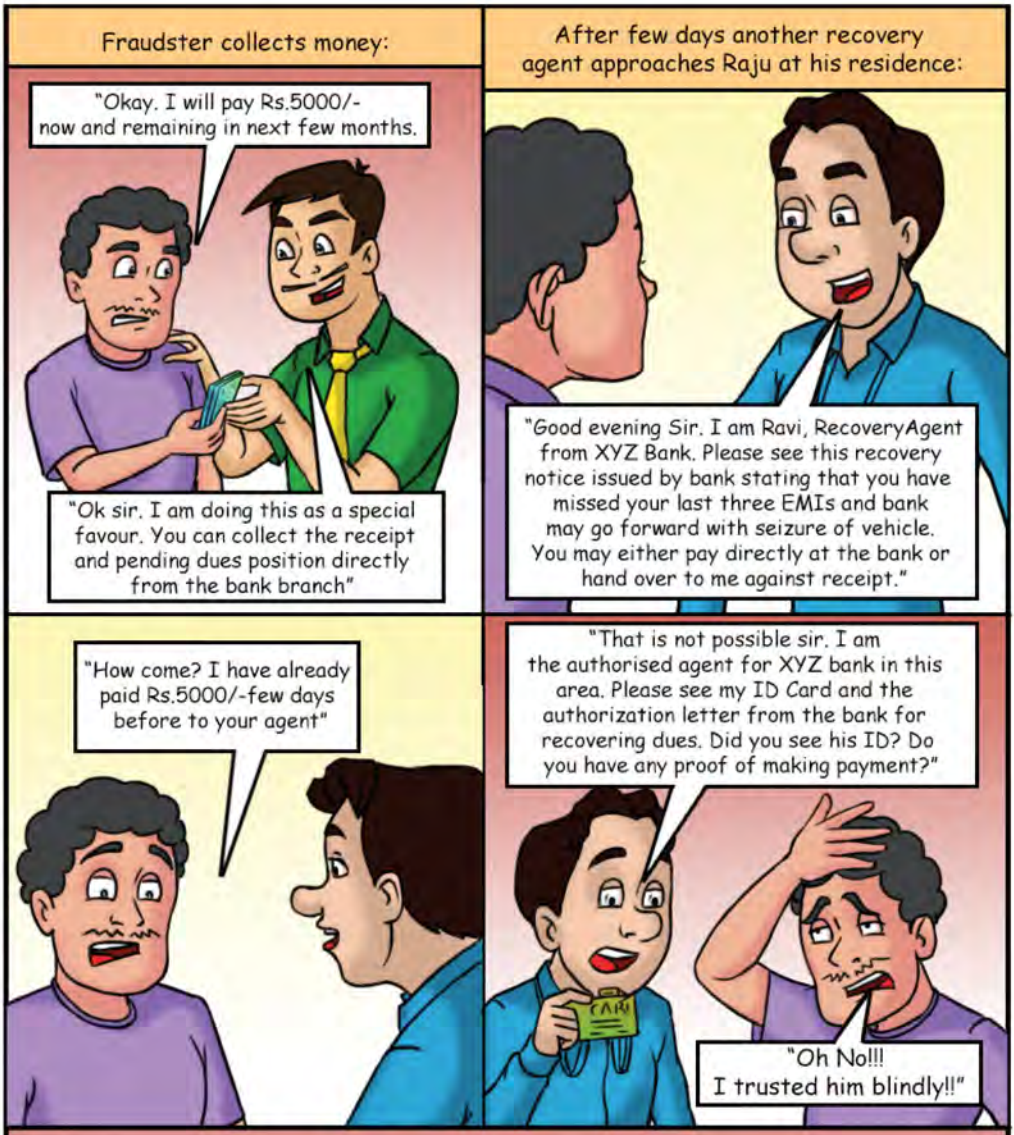
× Do not make a payment in advance when you are doubtful. If anybody asks for an advance payment, it is a matter of caution and one should go ahead with those transactions with requisite precaution.

21. FRAUDSTERS IN THE PRETEXT OF RECOVERY AGENTS



Do's:

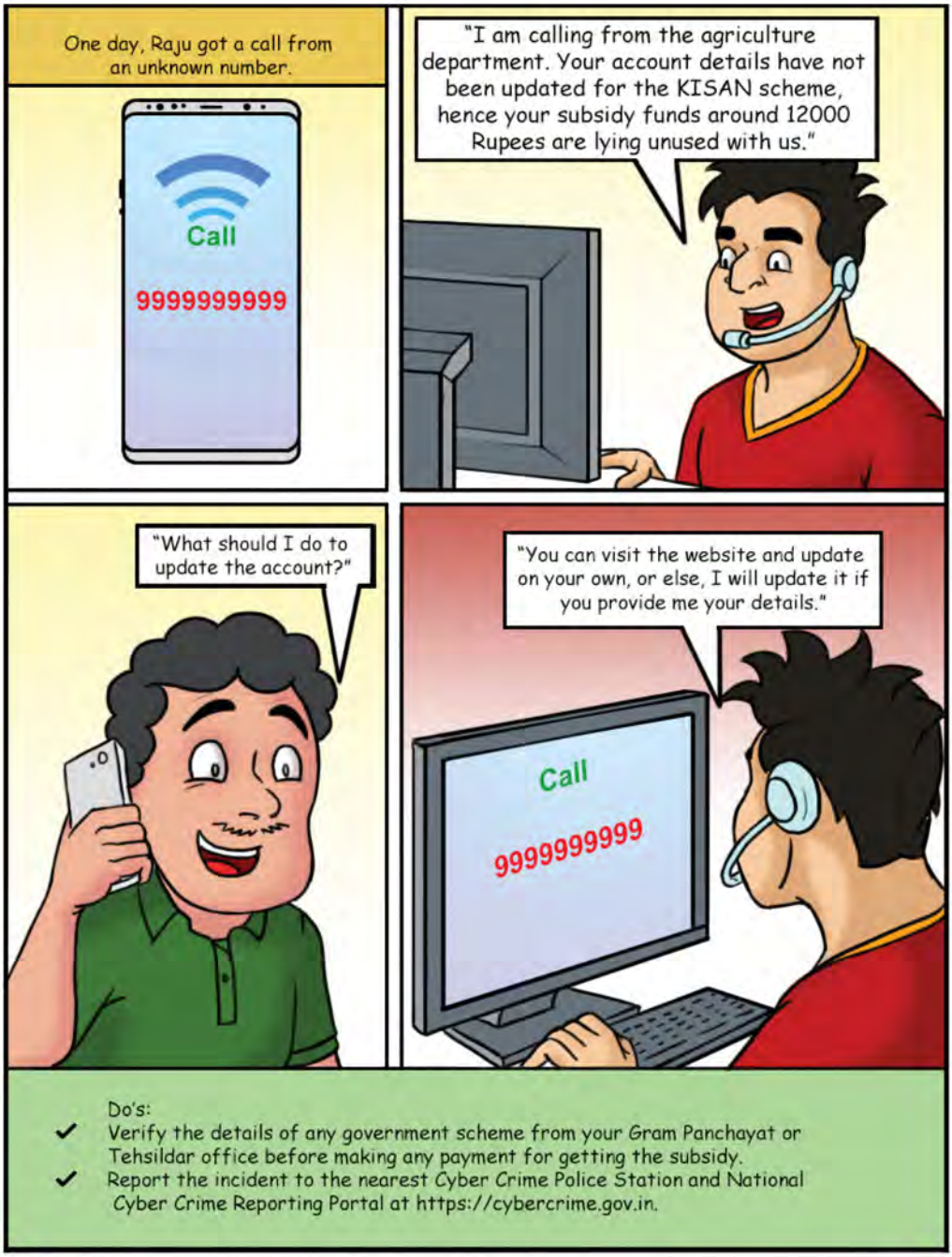
- ✔ Always ensure identification of Recovery Agents before making any payment / commitment. Check whether agent carries a copy of the recovery notice and the authorization letter from the bank along with the identity card issued to him by the bank or the agency firm. You can also cross verify with the home branch over phone.
- ✔ Report the incidence to the nearest Police Station and your home branch.



Don't's

✕ Never make any cash payments to bank/ recovery agents without proper acknowledgement of receipt.

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.

Raju provides the details of his bank account, debit card and shares the OTP to the fraudster

A few minutes later, Raju received an SMS from the bank saying Rs 25,000/- was debited from his bank account.

Raju was cheated under the pretext of registering for a social welfare scheme.

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.

23. MULTI-LEVEL MARKETING (MLM) SCAMS

Do's:

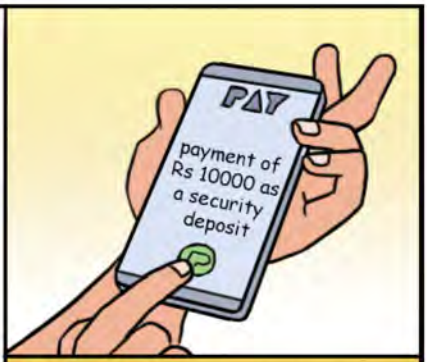
- ✔ Stay away from people trying to get you into these kinds of schemes.
- ✔ Verify the authenticity of the Multi Level Marketing scheme. Some of the network marketing schemes, like Ponzi scheme, Pyramid scheme etc., are illegal in India under the Direct Selling Guidelines, 2016 and the Prize Chits and Money Circulation Schemes (Banning) Act, 1978.
- ✔ Politely say no, even if the proposer of such a scheme is your friend or relative.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.

"This is a fantastic way to make money.I don't have to work every day as the agents recruited by me will be working on my behalf, and I will get commission on sales made by them."
"Yes, Raju. Therefore, I am visiting you. You may join my team as my agent."
Raju immediately filled up the form and agreed to become a direct selling agent of the multi-level marketing company.
However, sales were dismal and nonexistent. He could not accomplish the targets set by the company of recruiting 3 more agents, and he lost Rs 20000 as the products bought by him from the company also could not be sold. He did not get any mobile either.
Don't:
✕ Do not pay money to unknown companies and enrol in unknown schemes.

24. WORK FROM HOME SCAM

Do's:

- ✓ Beware of short URLs, information requested on Google forms from unknown sources.
- ✓ Look for poor spelling, grammar in emails, SMS, and portals.
- ✓ Be cautious of the links/forms asking for personal information.
- ✓ Always check the header of emails for verifying the genuineness of the offer or entity.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.



Raju makes the payment of Rs 10000 as a security deposit to the fraudster. The job progresses smoothly for a week. Raju kept receiving regular payments. He got 7000 Rs as remuneration.

In the next week, the agency started identifying mistakes; they consolidated the errors and produced a bill of Rs 1 lakh as compensation to the agency as per the terms and conditions of the contract signed by Raju initially.

Raju started receiving multiple harassment and recovery calls from different numbers in a single day.

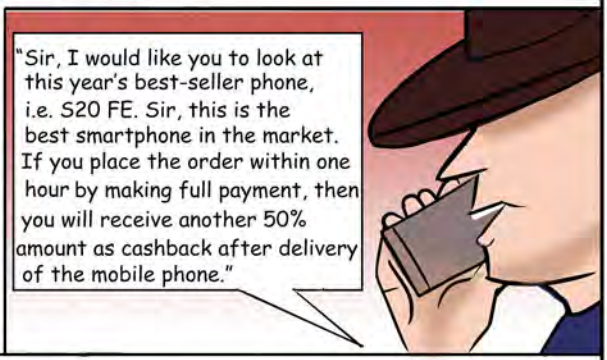
He got calls from 'lawyers', 'police' threatening legal action and then, terrified with all this, Raju paid Rs 1 lakh to the fraudster.

Don'ts:

- ✕ Never send sensitive, personal, or proprietary information (Aadhaar or Pan card) via email to unknown people.
- ✕ Never sign any online agreement before consulting a lawyer.
- ✕ Never pay to get a job, genuine firms never ask for deposits

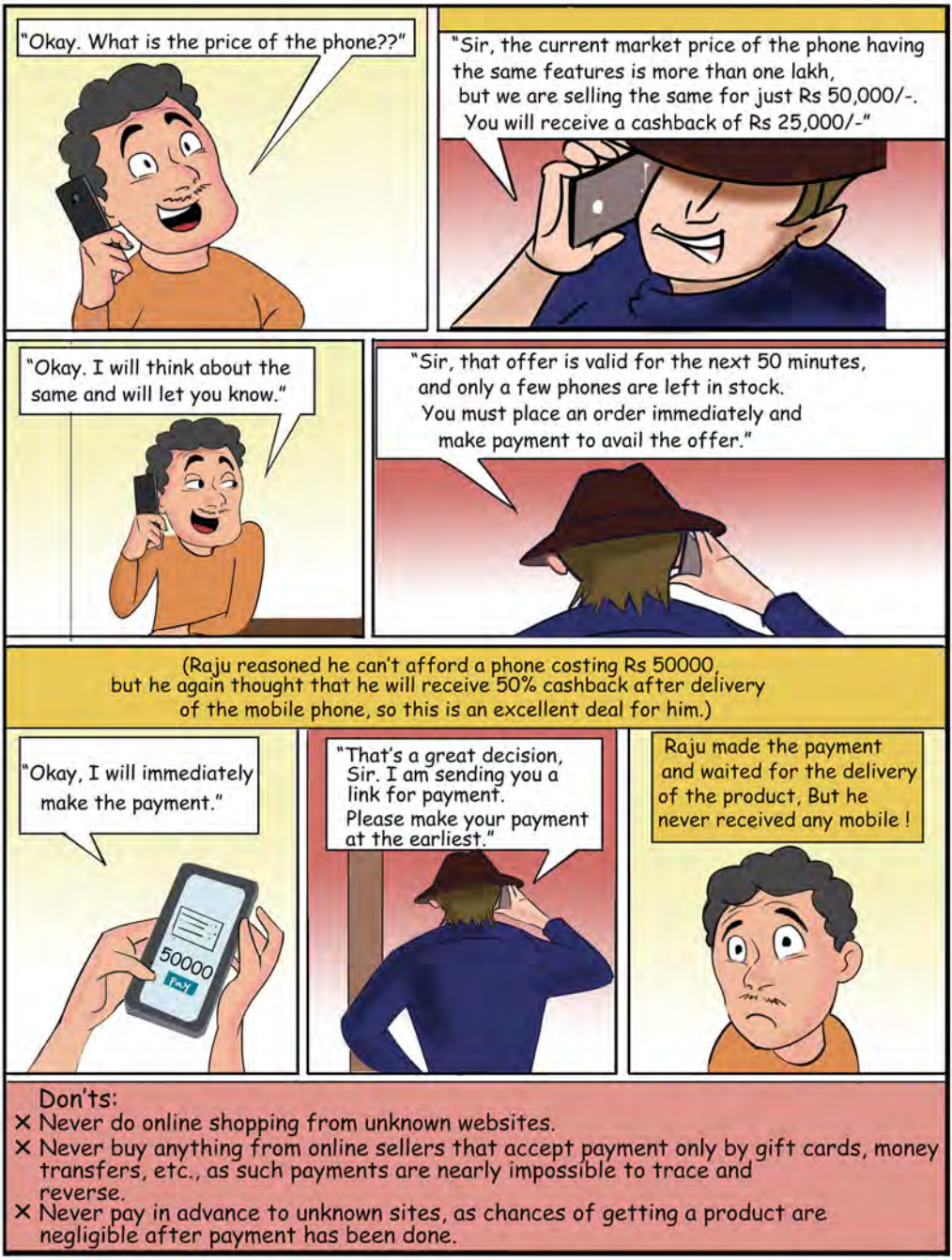
25. ONLINE SHOPPING FRAUD

One day, Raju received a message from an unknown number advertising mobile phones at a very cheap price.Out of curiosity, Raju clicks on the link and was surprised to see smartphones at a 50% discount.
Raju contacted the number mentioned on the website.



Do's:

- ✔ Always shop from secured websites. It is recommended to make sure the websites show a tiny lock icon or 'https', in the checkout browser, indicating transactions are secure.
- ✔ Report the incident to the nearest Cyber Crime Police Station & National Cyber Crime Reporting Portal at https://cybercrime.gov.in.

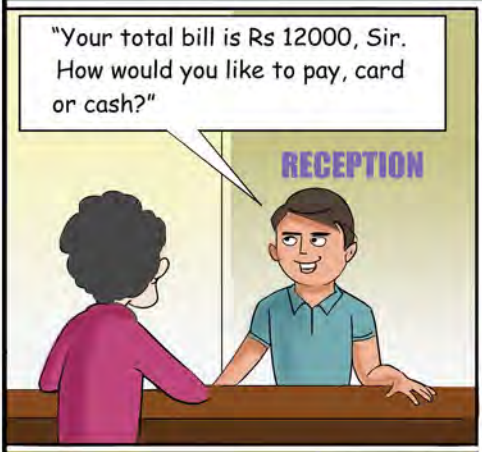


Don'ts:

- ✕ Never do online shopping from unknown websites.
- ✕ Never buy anything from online sellers that accept payment only by gift cards, money transfers, etc., as such payments are nearly impossible to trace and reverse.
- ✕ Never pay in advance to unknown sites, as chances of getting a product are negligible after payment has been done.

26. FRAUD USING PUBLIC WI-FI

It was a Sunday. Raju and his family were in the shopping mall. Raju bought some clothes and groceries and went to the reception to make the payment.



Raju initiated the payment but there was a network issue.

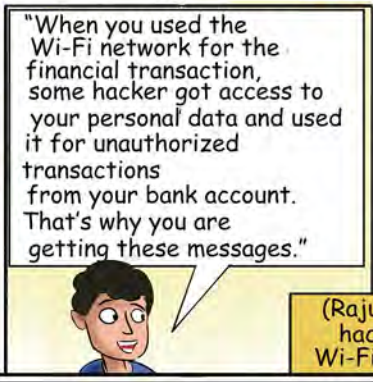
Do's:

- ✓ 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.

Raju connected to the free Wi-Fi and completed the transaction."

Raju was happy. His day was spent well. After some time, he started receiving SMS alerts from his bank. Rs 14000/- and Rs 10000/-were debited from your account.' Raju was confused.

The last transaction he made was Rs 12000/-at the mall, and these transactions were different. He told his son about the messages.

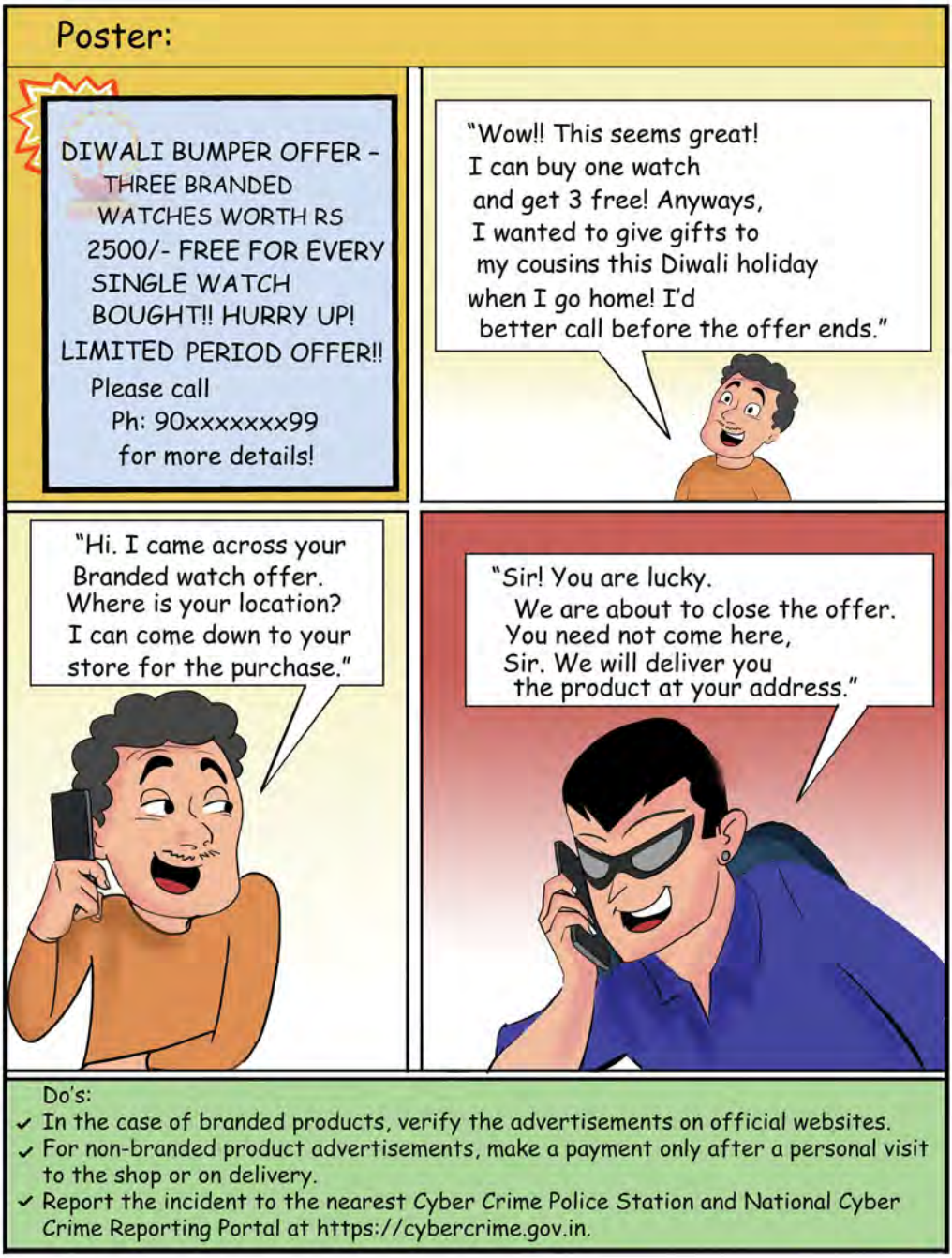


(Raju became a victim of hackers by using public Wi-Fi for financial transactions.)

Don'ts:

✕ Do not use public Wi-Fi, especially while doing financial transactions. It is easy to hack into a laptop or mobile device that is on a public Wi-Fi connection with no protection. Hackers can read your emails, steal passwords and other credentials.

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.

Raju indeed lost his money.

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

Raju is a humble farmer trying to make both ends meet.
One day, he received a call from a stranger.

"Hello, Mr Raju. We are calling from xyzzy Pvt Ltd. We have introduced a scheme for farmers in your region. You have been found eligible for availing a loan from our company at a subsidized rate."

"Oh! Okay. That would be helpful. What is the offer?"

"We offer special loans up to Rs 5 lakhs at an interest of just 3%! For availing this loan, you need to share your bank account and Aadhaar details for verification."

"Okay. I will think about the same and will let you know."

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.

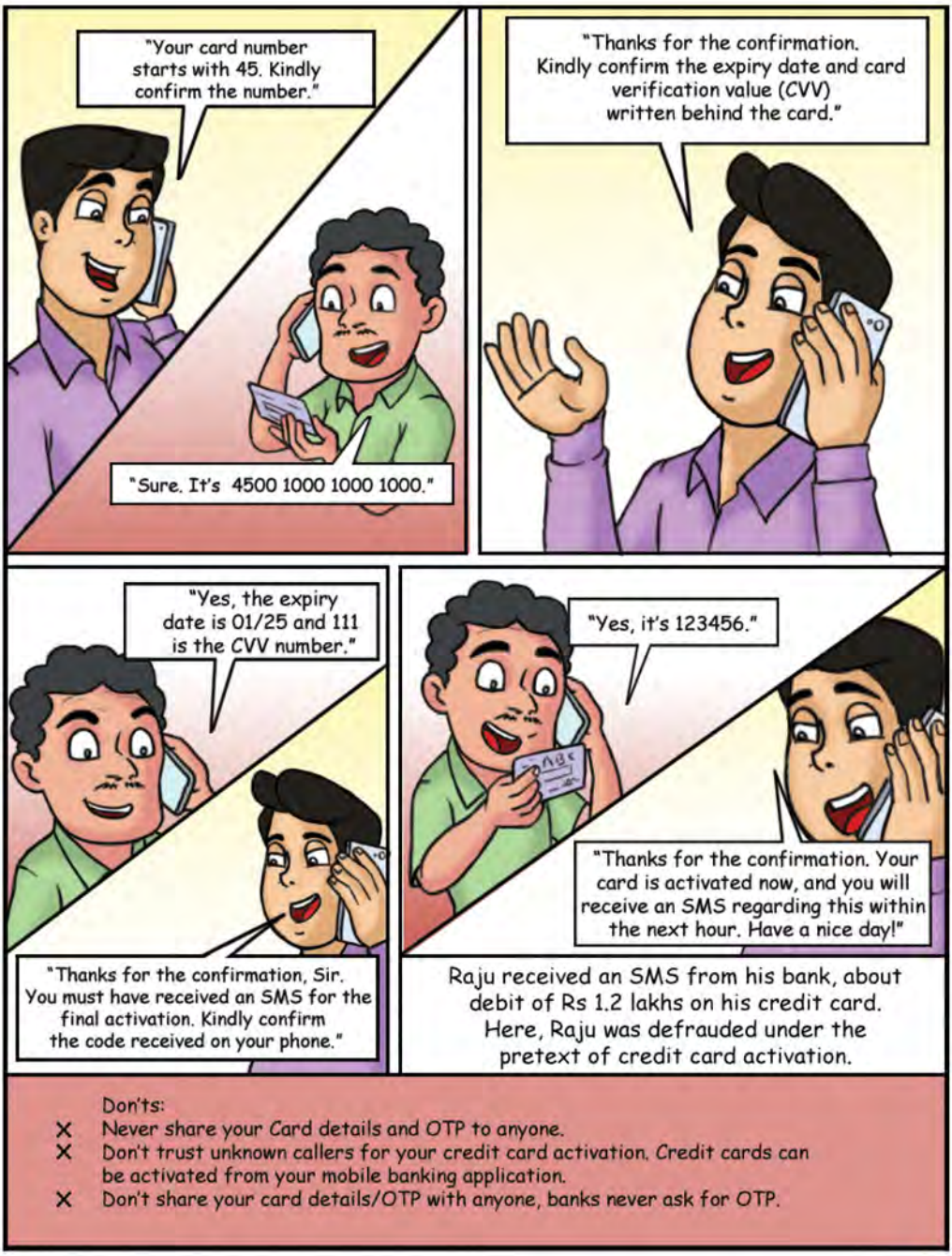
Don't:

✕ 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.

29. CREDIT CARD ACTIVATION FRAUD

Do's:

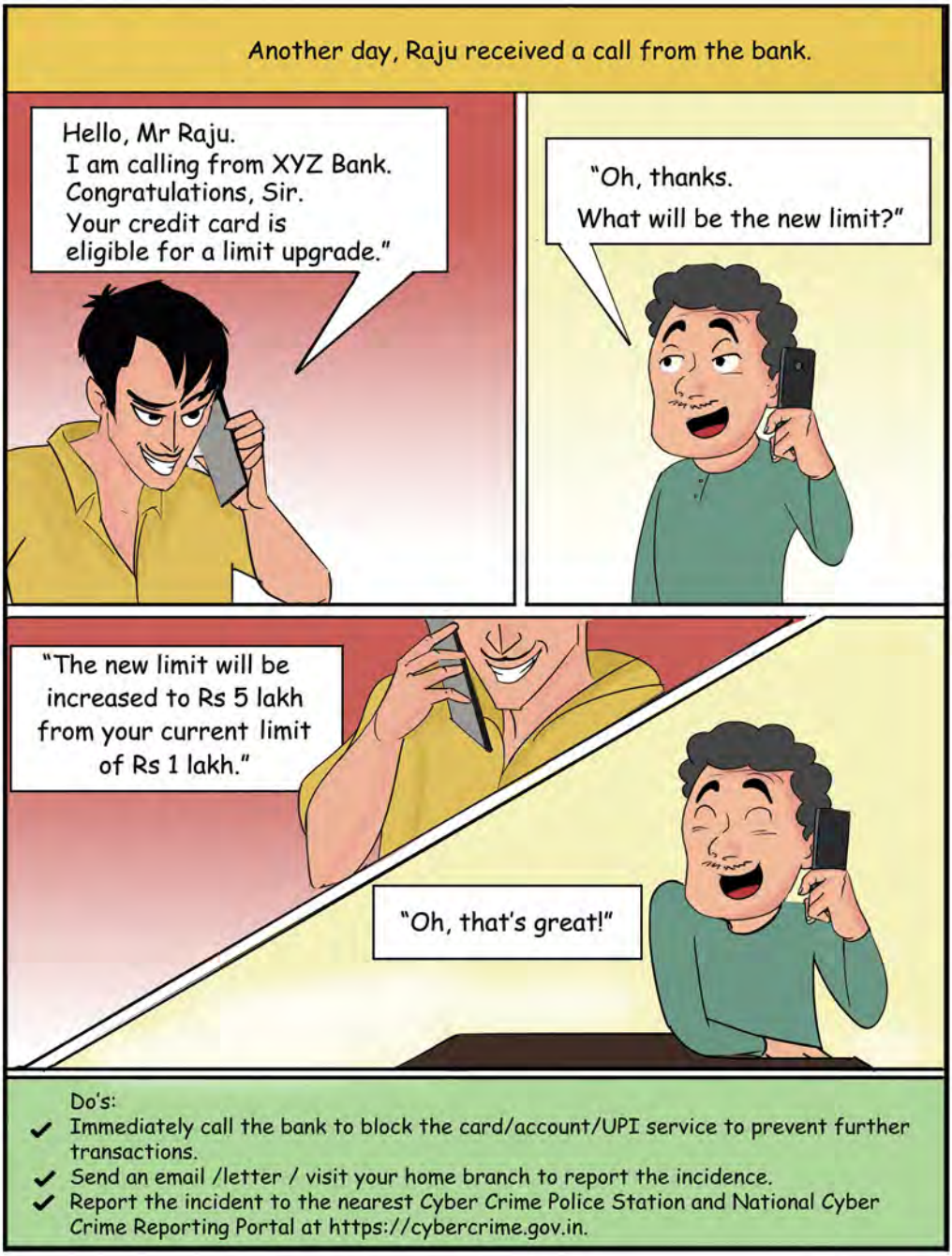
- ✔ Call the bank to block the card/bank account/UPI services to prevent further monetary loss.
- ✔ Send an email /letter / visit your home branch to report the incidence.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.



Don'ts:

- ✕ Never share your Card details and OTP to anyone.
- ✕ Don't trust unknown callers for your credit card activation. Credit cards can be activated from your mobile banking application.
- ✕ Don't share your card details/OTP with anyone, banks never ask for OTP.

30. CREDIT CARD LIMIT UPGRADATION FRAUD



Do's:

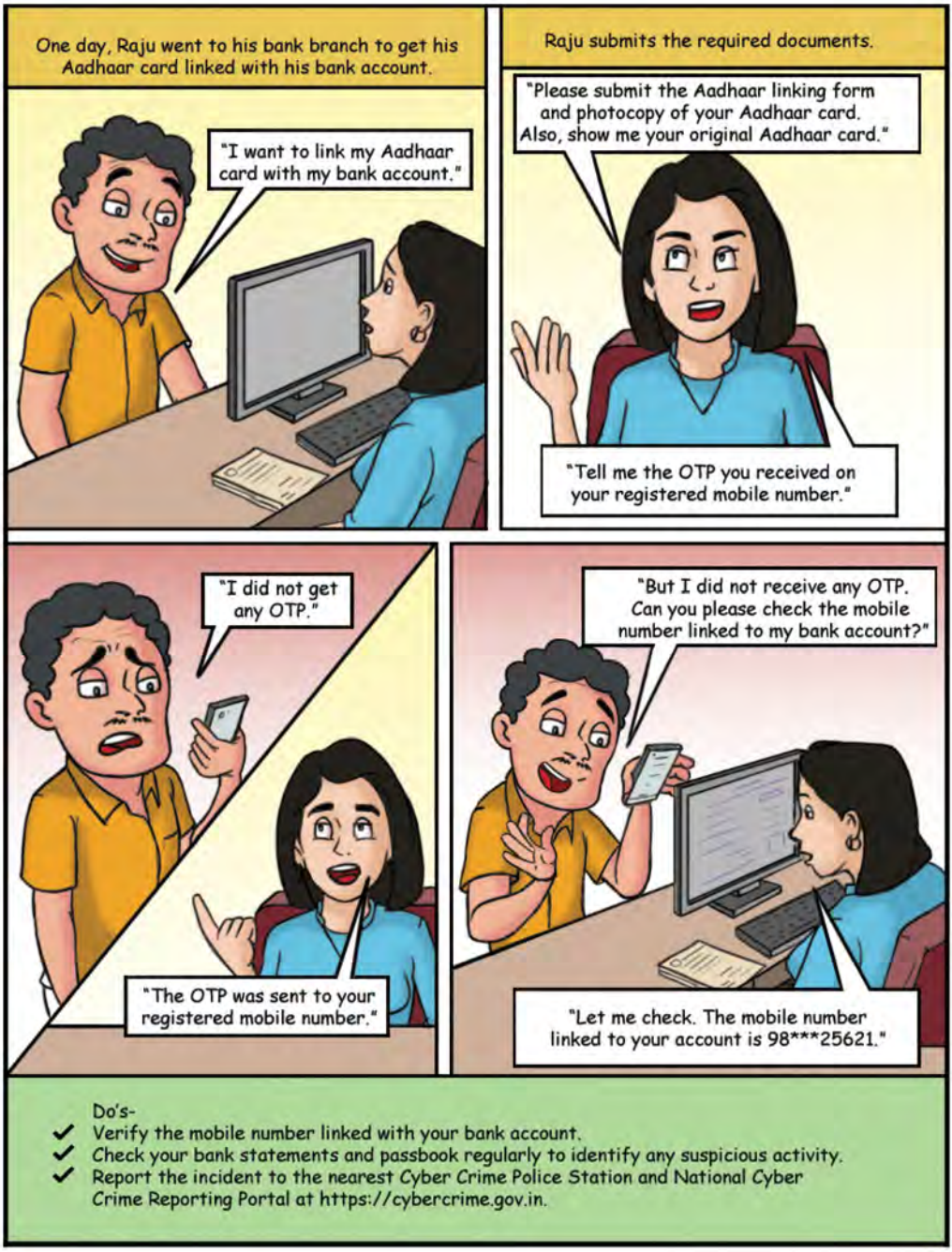
- ✔ Immediately call the bank to block the card/account/UPI service to prevent further transactions.
- ✔ Send an email /letter / visit your home branch to report the incidence.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.

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.

31. SAFE GUARDING YOUR AADHAAR CARD



Do's-

- ✔ Verify the mobile number linked with your bank account.
- ✔ Check your bank statements and passbook regularly to identify any suspicious activity.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.

"But this is not my mobile number."
"You visited the bank last week."
"Last time when I visited the bank to submit my KYC form, a gentleman in the bank helped me fill the form and submitted it for me."
"The form you submitted may have his mobile number, and your bank account is linked with that number. He can easily misuse your bank account. You should have checked that form before submitting."
"I had no idea about this. I made such a big mistake. What can I do now?"
"Please submit a form for changing your registered mobile number"
Don'ts-
✕ Don't share your confidential details like Aadhaar and bank account details with strangers.

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.

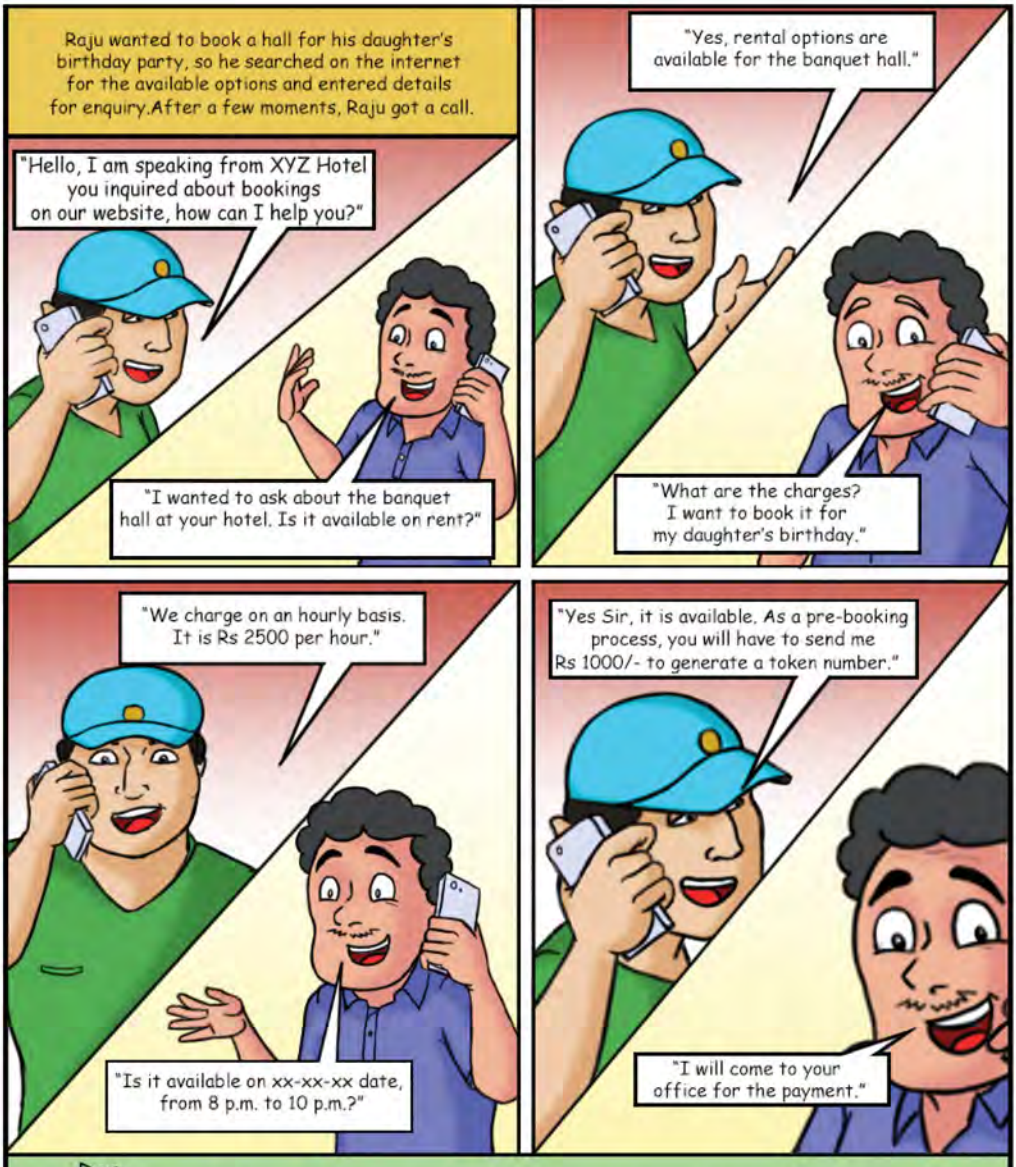
(The moment Raju entered his UPI PIN, an amount of Rs 20,000/- was debited from his account. Raju tried calling the Fraudster but was unable to connect.)

Don'ts-

× Don't believe the caller blindly; one should verify the company's official website to check the authenticity of the offer.

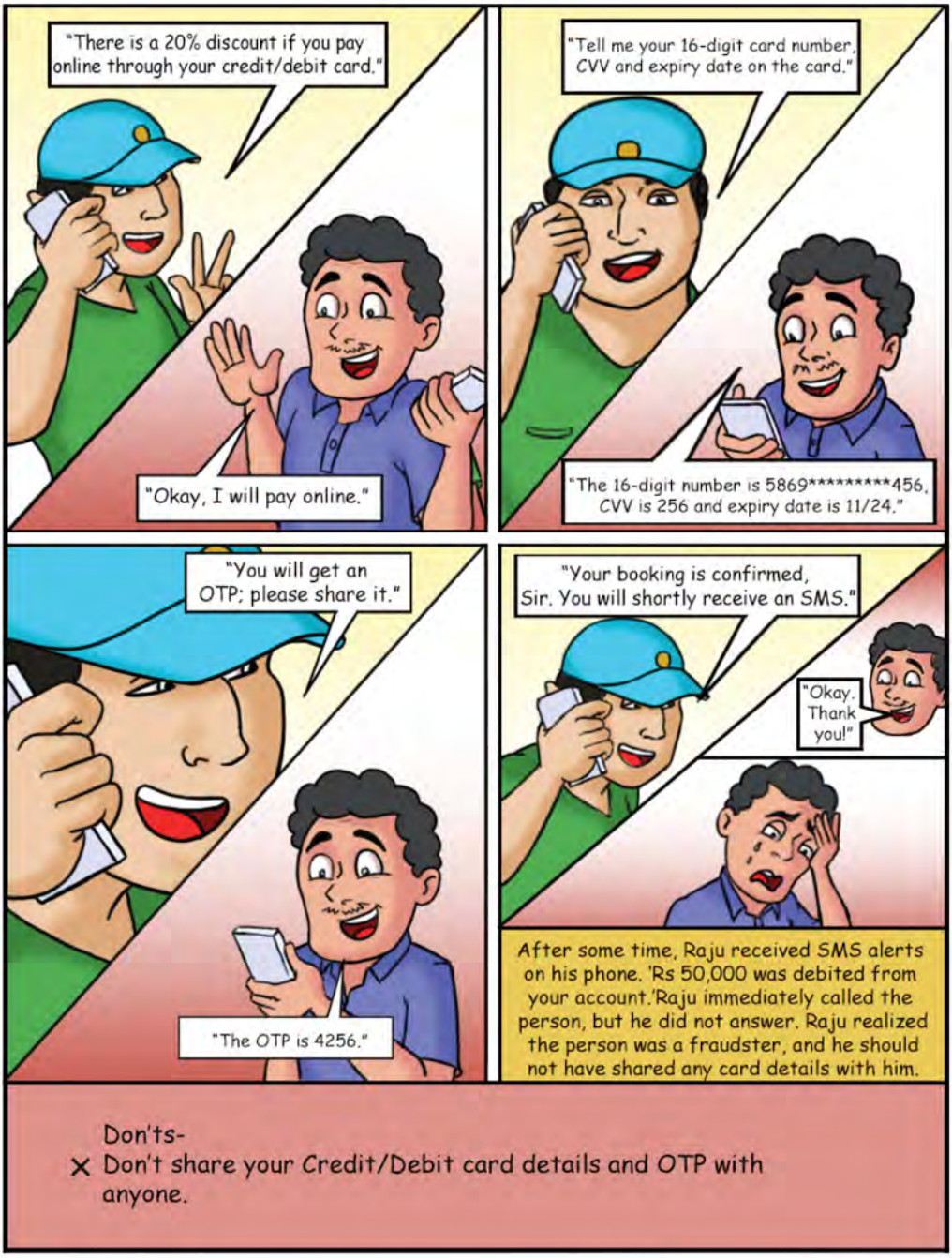
× Don't enter or share UPI PIN for receiving payments as it is required only for sending payments.

33. DISCOUNT FRAUD



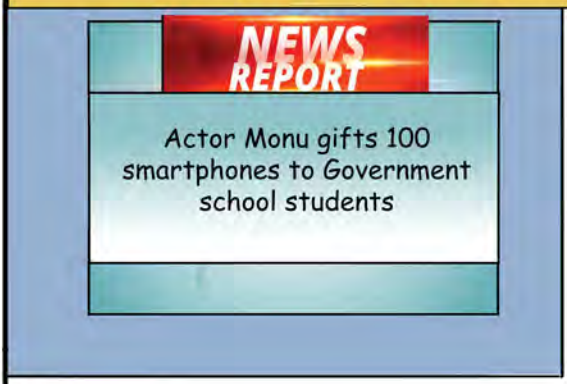
Dos-

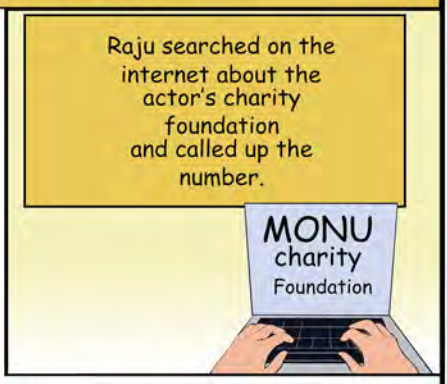
- ✓ Always verify the authenticity of a person/institution offering any deal or offer.
- ✓ OTP SMS will have other details like amount / merchant name / beneficiary name of intended transaction. Always read the OTP SMS alerts thoroughly before use.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in.


"There is a 20% discount if you pay online through your credit/debit card."
"Okay, I will pay online."
"Tell me your 16-digit card number, CVV and expiry date on the card."
"The 16-digit number is 5869*********456, CVV is 256 and expiry date is 11/24."
"You will get an OTP; please share it."
"The OTP is 4256."
"Your booking is confirmed, Sir. You will shortly receive an SMS."
"Okay. Thank you!"
After some time, Raju received SMS alerts on his phone. 'Rs 50,000 was debited from your account.'Raju immediately called the person, but he did not answer. Raju realized the person was a fraudster, and he should not have shared any card details with him.
Don'ts-
✕ Don't share your Credit/Debit card details and OTP with anyone.

34. CHARITY FRAUDS

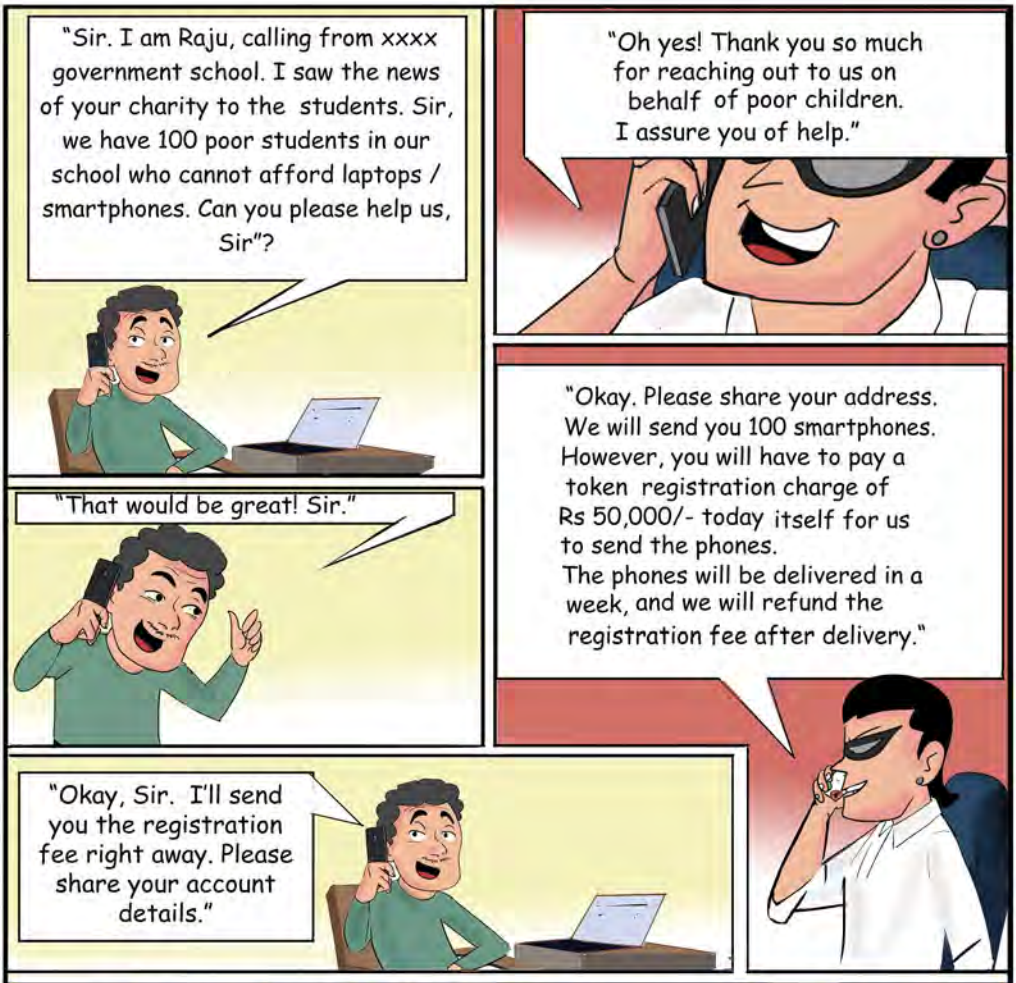
Raju is a Government school teacher.
He came across a news report that Actor Monu
was gifting smartphones to government school students.





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

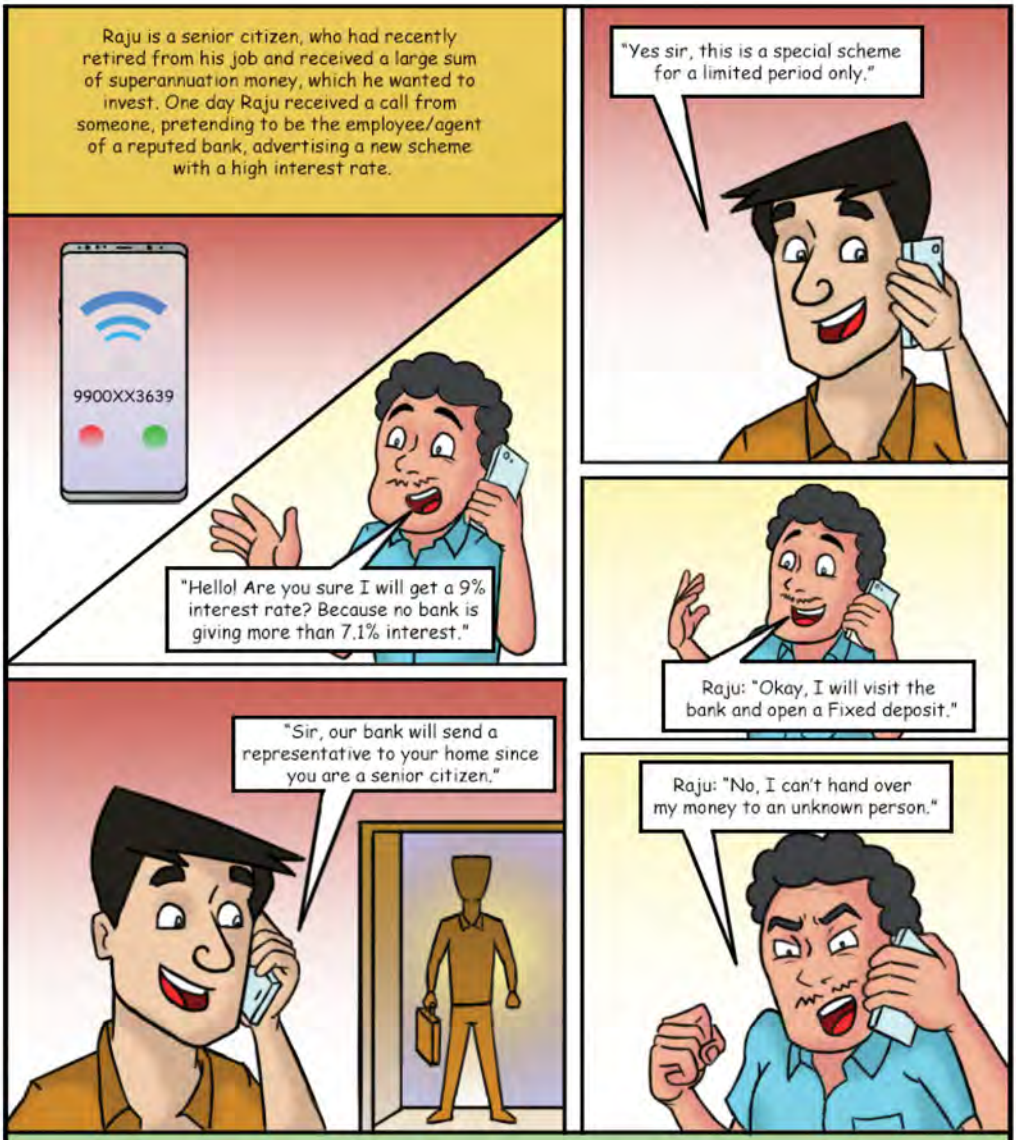


Raju transferred the funds, but he later came to know that no such mobile phones were donated to government school students. Raju realised that he had been duped by fraudsters under the pretext of charity.

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.

35. OVERDRAFT AGAINST FD



Do's:

- ✔ Check all documents before signing.
- ✔ Prefer visiting the bank branch or performing transactions over internet banking with the assistance of known person.
- ✔ Report the incident to the nearest Cyber Crime Police Station or National Cyber Crime Reporting Portal https://cybercrime.gov.in in case of cybercrimes.

The fraudster visits Raju's home to collect the cheque and takes signatures on different forms, which Raju does not check before signing.

After a day, the fraudster visits the branch as a representative of Raju and deposits the cheque for creating a fixed deposit. However, he gave fake fixed deposit receipts to Raju and kept the original ones with himself.

The fraudster poses as a representative of Raju and uses the overdraft form signed by Raju, which has fraudster's account number for credit of the overdraft.

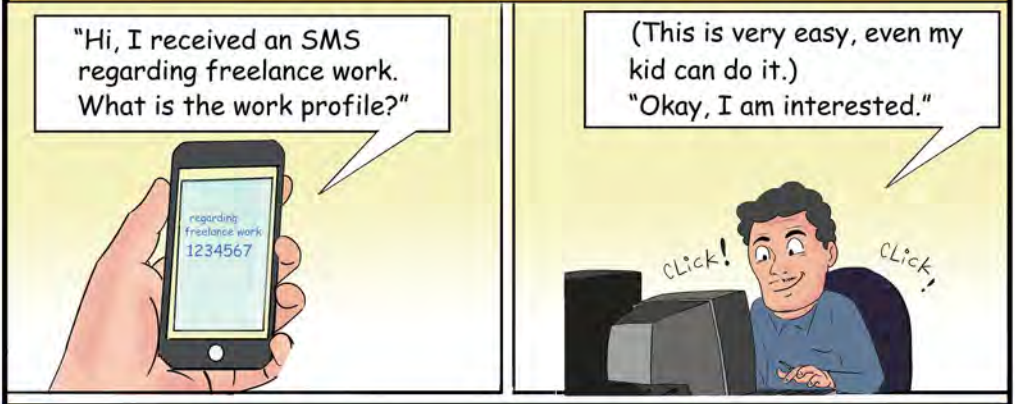
After a day, Raju got an SMS regarding an overdraft issued against the FD and upon visiting the branch, he was shocked to know that the FD receipt he had received was fake.

Don'ts:

× Do not hand over important documents/cheques to unknown person.

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."

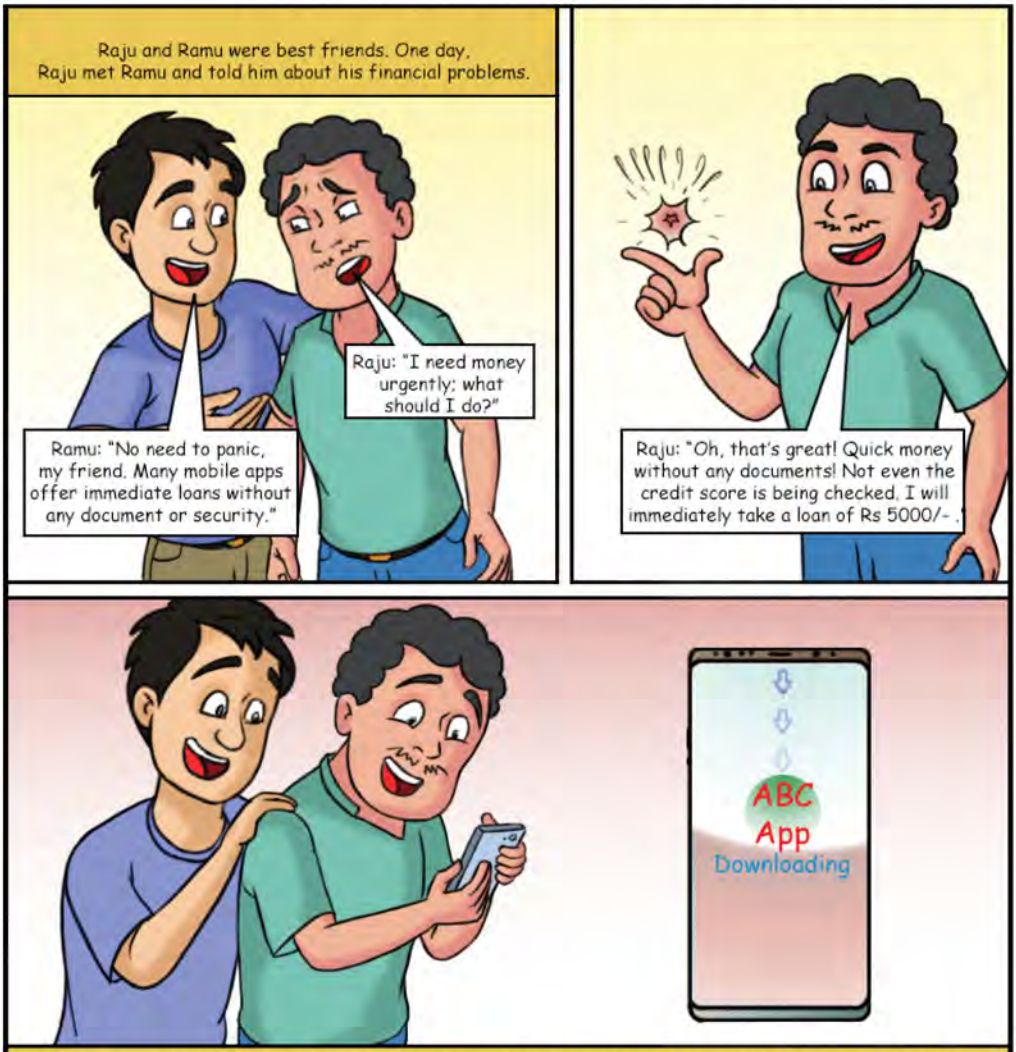
After a few days, Raju received SMS alerts stating Rs 50,000 was debited from his account Raju had no clue how his account was compromised or money was debited.

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.

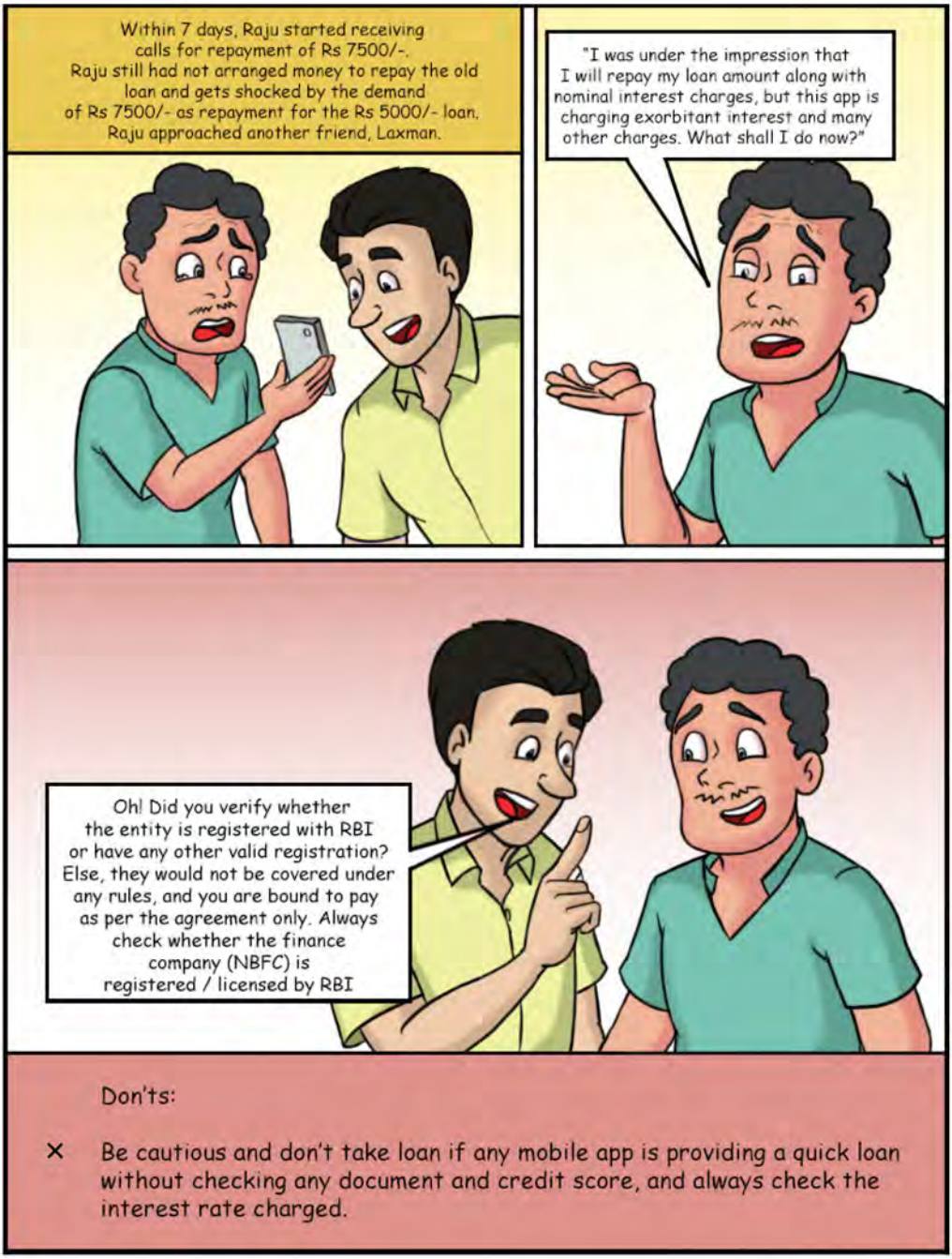
37. ILLEGAL LOAN FINANCING APPS WITH EXORBITANT INTEREST RATES AND HARASSMENT TACTICS



Raju downloads a mobile app without verifying whether the entity providing loan is registered one. He gets Rs. 5000/- in his Bank account within no time.

Do's-

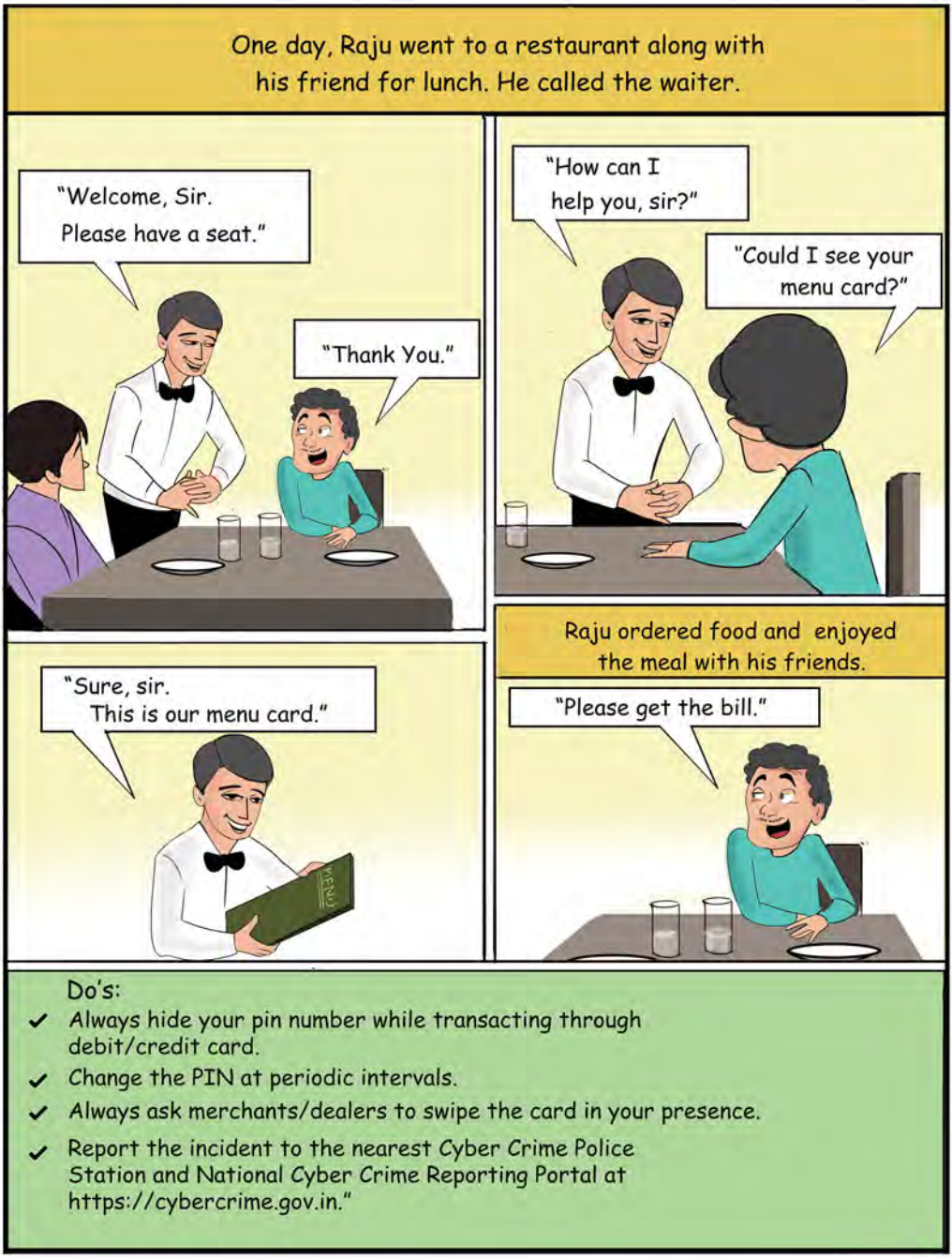
- ✓ Be cautious while downloading any app and providing the app permission to access data from your mobile phone.
- ✓ Always check the registration status of the company/NBFC whose application is being used to provide loan and terms and conditions before availing loan from that NBFC at https://www.rbi.org.in/Scripts/BS_NBFCList.aspx.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in."



Don'ts:

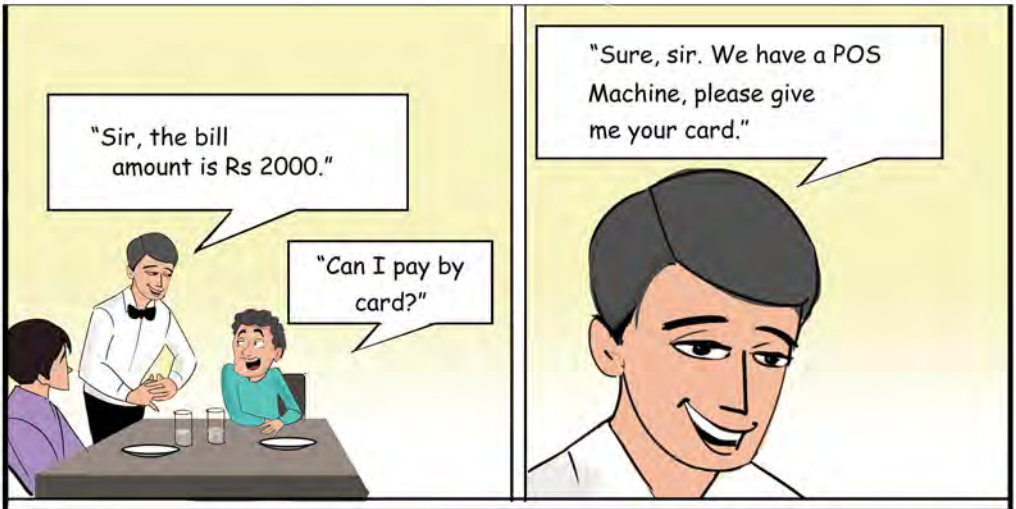
× Be cautious and don't take loan if any mobile app is providing a quick loan without checking any document and credit score, and always check the interest rate charged.

38. CARD CLONING AT MERCHANT OUTLETS

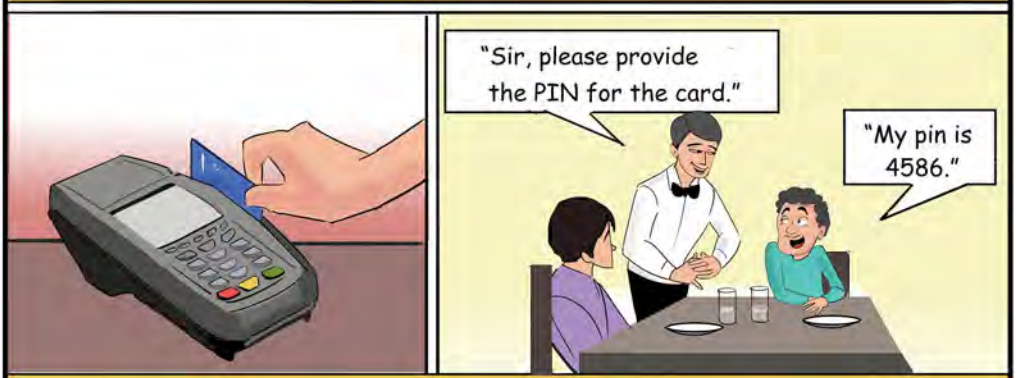


Do's:

- ✔ 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.

39. FRAUD THROUGH DETAILS SHARED WITH KNOWN PERSON/FAMILY/RELATIVES

Raju is a very friendly and helpful person, but he is ignorant when it comes to protecting his financial credentials or bank details. One day Raju received a call from his friend, Keshav.

Raju shared a photo of his credit card with his friend.

Raju's friends always use his cards to avail discounts offered by e-commerce websites, and he often sends his card details to his friends over the phone.

Do's:

- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in."
- ✓ Change the PIN at periodic intervals.

After a month, Raju received an SMS on his mobile number and was unable to figure out where the card was used.

Raju registered a complaint with the bank. The bank further informed him that the disputed transactions were done at an online merchant site.

Keshav: "Raju, just a few days back, I lost my mobile phone, and my phone has your card details. I am afraid that could have led to these transactions."

Raju realised that he himself had never done any payment at the online site, but he had shared his card details with his friends. Raju immediately contacted all his friends, but everyone informed him that they did not do the transaction.

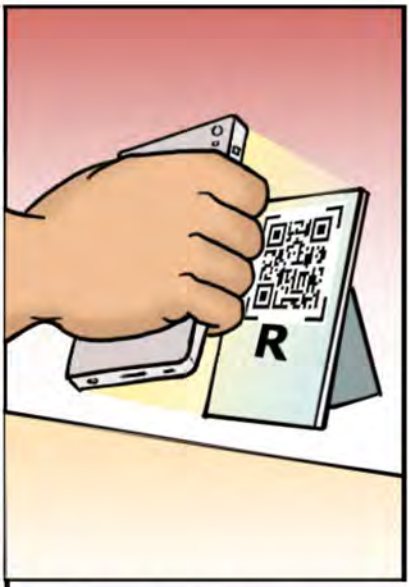
Don't:

✕ Do not share your card details over social media or messaging apps even if the recipient is your friend / relatives / family.

40. PAYMENT SPOOFING APPLICATIONS.

Do's:

- ✔ Always check/confirm transactions by checking your bank account whenever a transaction is done through UPI.
- ✔ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in."



The customer scanned the code under a fake XYZ app. He generated a fake payment intimation/screenshot and showed it to Raju.
Fraudster: "The payment is done."

(on seeing the screenshot of the fraudster)

At the end of the day, Raju cross-checked his shop account for reconciliation and found that one payment was not yet received in his account. Now he realized that he was duped by showing a fake screenshot.

On this spoofing, Raju cannot even complain to the bank or give a fraud report, as the actual fund transfer never happened, and Raju does not have any details of the customer.

Don't:

✕ Don't conclude financial transaction without actual receipt of fund.

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**