



Raju & The Forty Thieves



*A Booklet on Modus
Operandi of
Financial Fraudsters*

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





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!

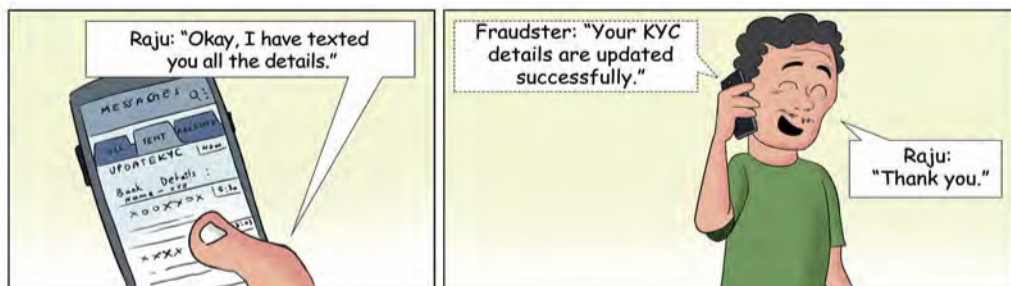


INDEX

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



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

One day, Raju received a call.

Fraudster: "Hello Sir, I am calling from XYZ Bank."

Raju: "Hi, what is the matter?"

Fraudster: "This is regarding your insurance policy. Your policy is activated, and you need to pay Rs18000 as a premium."

Raju: "No! I don't have any insurance with XYZ bank."

Fraudster: "Sir, it got activated as a promotional offer at a very low fee. But if you don't need it, I will deactivate it."

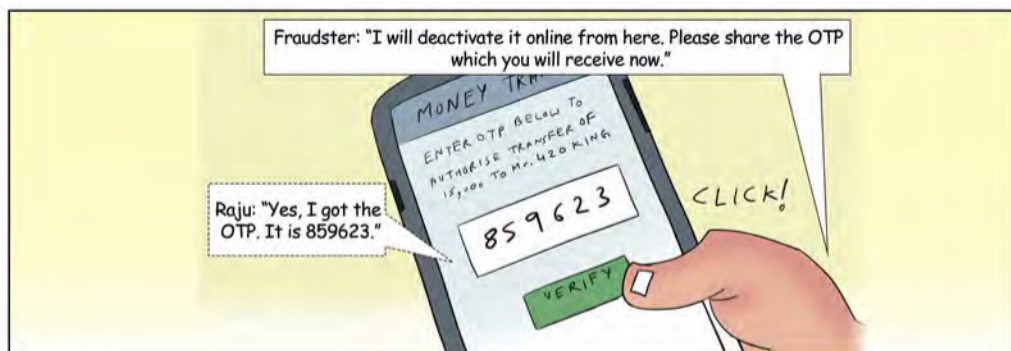
Raju: "I don't understand how you activated the policy without my consent, and why should I trust you?"

Fraudster: "Sir, I am calling you directly from the XYZ Bank customer care. I have all your details like Name, Address, Card details, DOB, Company Name and Designation."

Raju: "Okay, so tell me how to deactivate the policy?"

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

Raju wanted to dispose of sofa set. He posted the advertisement on the website which is an online marketplace for second-hand goods.

Click!

For SALE

Immediately after posting the advertisement, there was an enquiry from a fraudster offering to pay Rs 15,000/- for the sofa set. Raju felt very happy after getting an offer.

Fraudster: "I will pay online before picking up the furniture."

Raju: "Okay. Fine."

Fraudster: "Please share your account number."

Raju: "My account number is 123xxx67."

Fraudster: "I will first send Rs 10/- before making the final payment to verify the account."

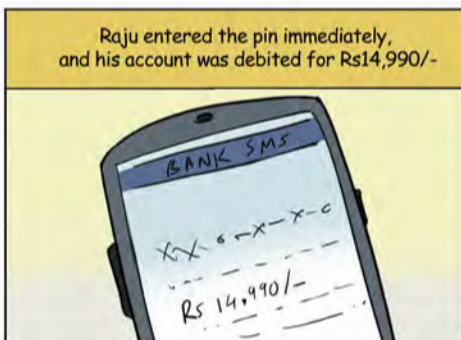
The fraudster sent Rs10/- to Raju's account and asked for confirmation for the final payment.

Raju: "Okay, I got it."

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.



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.

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

Fraudster: "Thank you, Mr Raju. Your annual fee is waived off. Have a great day!"



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.

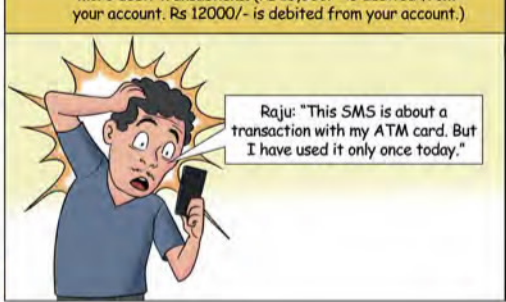
5. ATM CARD SKIMMING FRAUD

Raju receives his monthly salary in his account. He visits an ATM to withdraw money for his monthly expenses.



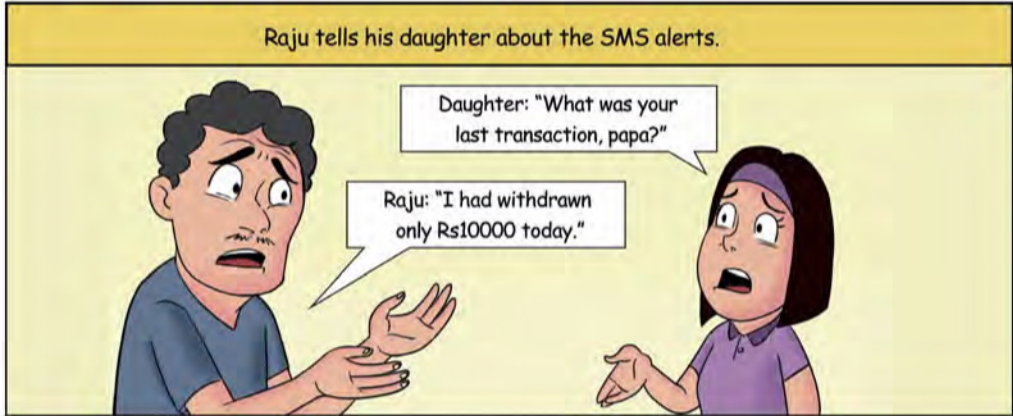
Raju withdraws the money, and he gets an SMS alert for his transaction.

After a few hours, Raju gets SMS alerts for a few more debit transactions. (Rs 15,000/- is debited from your account. Rs 12000/- is debited from your account.)



Raju: "This SMS is about a transaction with my ATM card. But I have used it only once today."

Raju tells his daughter about the SMS alerts.



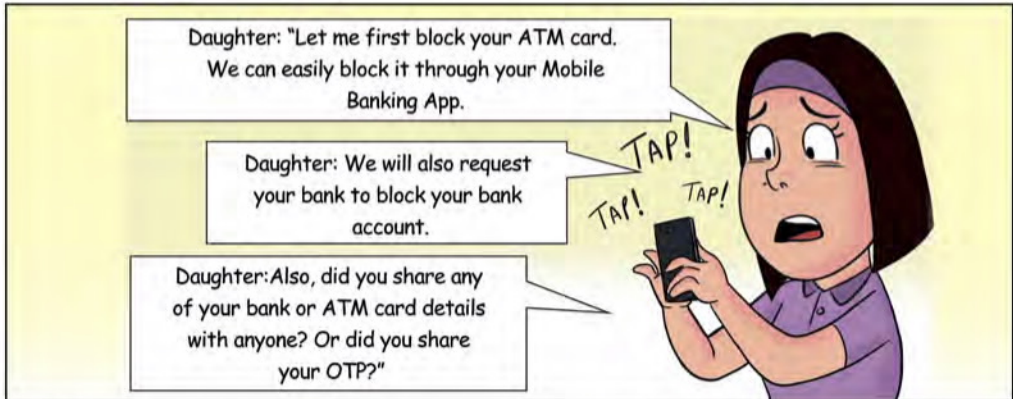
Daughter: "What was your last transaction, papa?"

Raju: "I had withdrawn only Rs10000 today."

Daughter: "Let me first block your ATM card. We can easily block it through your Mobile Banking App."

Daughter: We will also request your bank to block your bank account.

Daughter: Also, did you share any of your bank or ATM card details with anyone? Or did you share your OTP?"

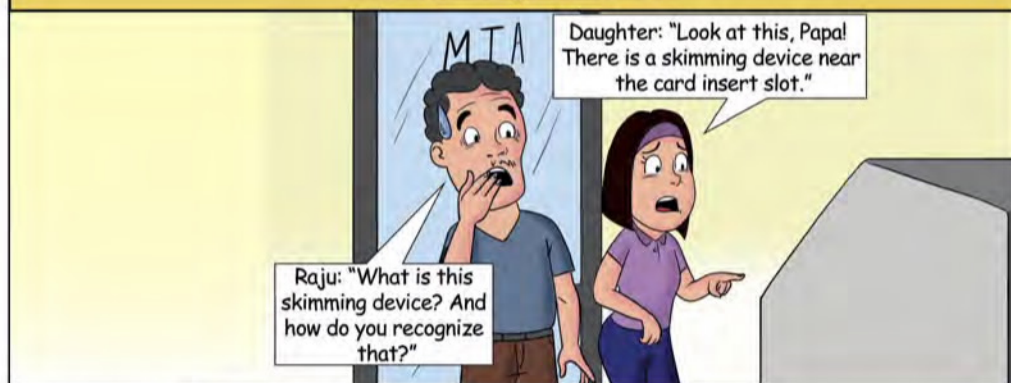


Do's:

- ✓ 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>)



Both of them go to the ATM.



Raju files a complaint with his bank.



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

Fraudster: "Hello Sir! Good Morning.
 I am calling from ABC Gaming Corporation. We are delighted to offer you a cash reward for playing an online game."



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

Fraudster: "Sir, I am an employee of the company which makes online games, and this is a beta version of the new game we have developed. We need feedback from users before launching the game to the public. So, we are inviting gamers to download this app, play games and give us feedback for improvement. We will be giving you Rs 10,000/- for this."



Fraudster: "Sir, I have shared the link to download the app. You can log in with the User Id-XXXXXX@ABC.com and password- MNOPQRS."



Raju: "Oh Wow! I will get a cash reward for playing the game. From where do I install this game?"

Raju: "I have successfully downloaded the app. What should I do next?"

Fraudster: "Sir, you will see a code for logging into the app. Please share it with us."

Raju: "What? Code? Is this like an OTP for financial transactions?"



Do's:

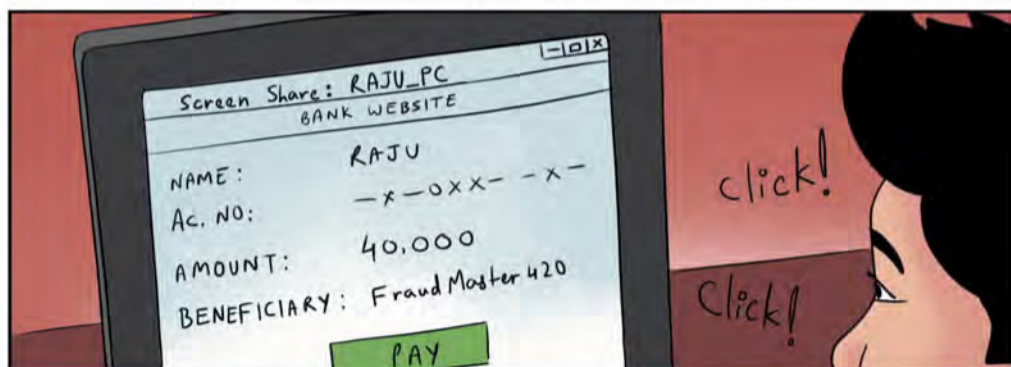
- ✓ Verify the authenticity of the offer on the official website of the entity concerned.
- ✓ Install antivirus/spam blocking software on your mobile phone.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Fraudster successfully installed the screen-sharing app in Raju's mobile and gained access to his phone. He could read the messages on Raju's mobile and track his keypad.

Fraudster: "Sir! We would be giving you Rs 10000 for participation but before that please pay Rs 10 to the account 12345 through net banking to activate the account. Please call me once done."

Raju thinking that it was just a matter of Rs 10/- transferred the amount through Net Banking. Soon he received debit messages of Rs 35000, Rs 20000 and Rs 40000.



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.



Raju: "What has happened to my mobile! There is no network, and I am not able to make calls, send messages, etc."



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.

Fraudster: "You will get the payment link on your phone now. Please click and make the payment."



Raju - "Yes, I got the payment link. I will pay the amount now."



Click!

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 transaction.

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)

Fraudster: "Hi, I saw your car advertisement on the platform. I really liked it, and I am interested in buying your car."



Fraudster: "Oh! Don't worry about the price. I am an army personnel, and I am about to retire in a month. My son wants to purchase a car, and he is insisting on buying this one only."

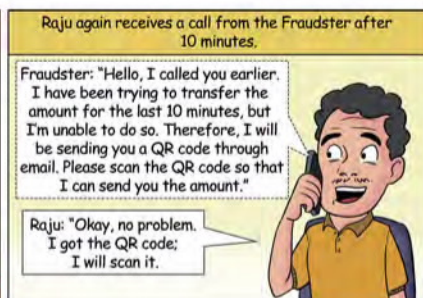
Raju: "Glad you liked it. My car is in excellent condition. I am buying a new car, so I am selling this one. I won't negotiate the price."

Raju: "That's great! I guess you want to check the car before buying it."

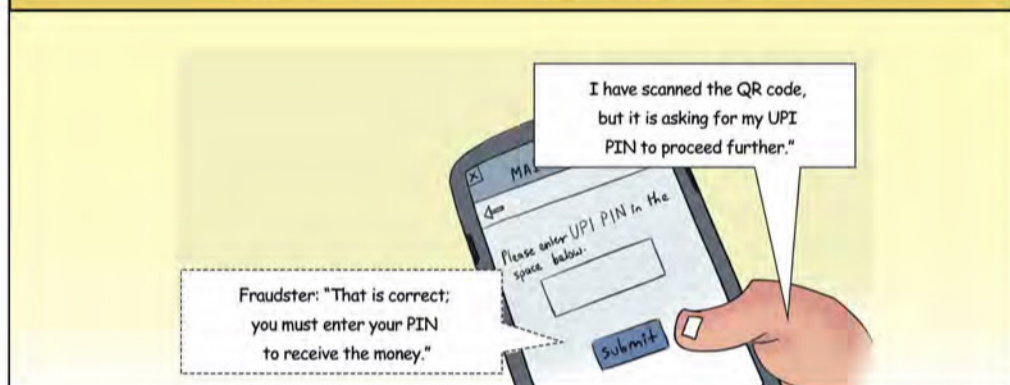
Fraudster: "Sure, we want to inspect the car, but before that, I will send you a token amount as I don't want to lose the offer."

Do's:

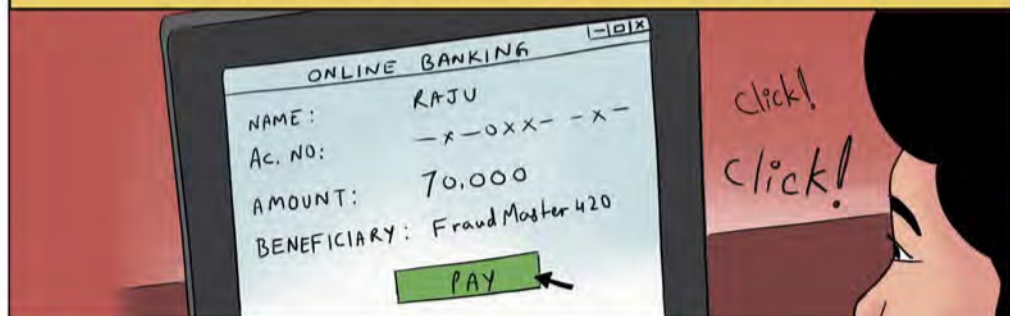
- ✓ Educate yourself about QR codes before using them.
- ✓ Report the transaction immediately to your bank.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Raju scans the QR code and receives a pop-up request for UPI PIN.



Raju believed him and entered his UPI PIN. Subsequently, his account got debited with Rs 70,000. Raju received the SMS alert of the debit. He panicked, so he tried calling the fraudster, but his phone was switched off by then.



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



Soon Raju got accustomed to using social media: he started posting pictures, liking posts, sending friend requests and messages.

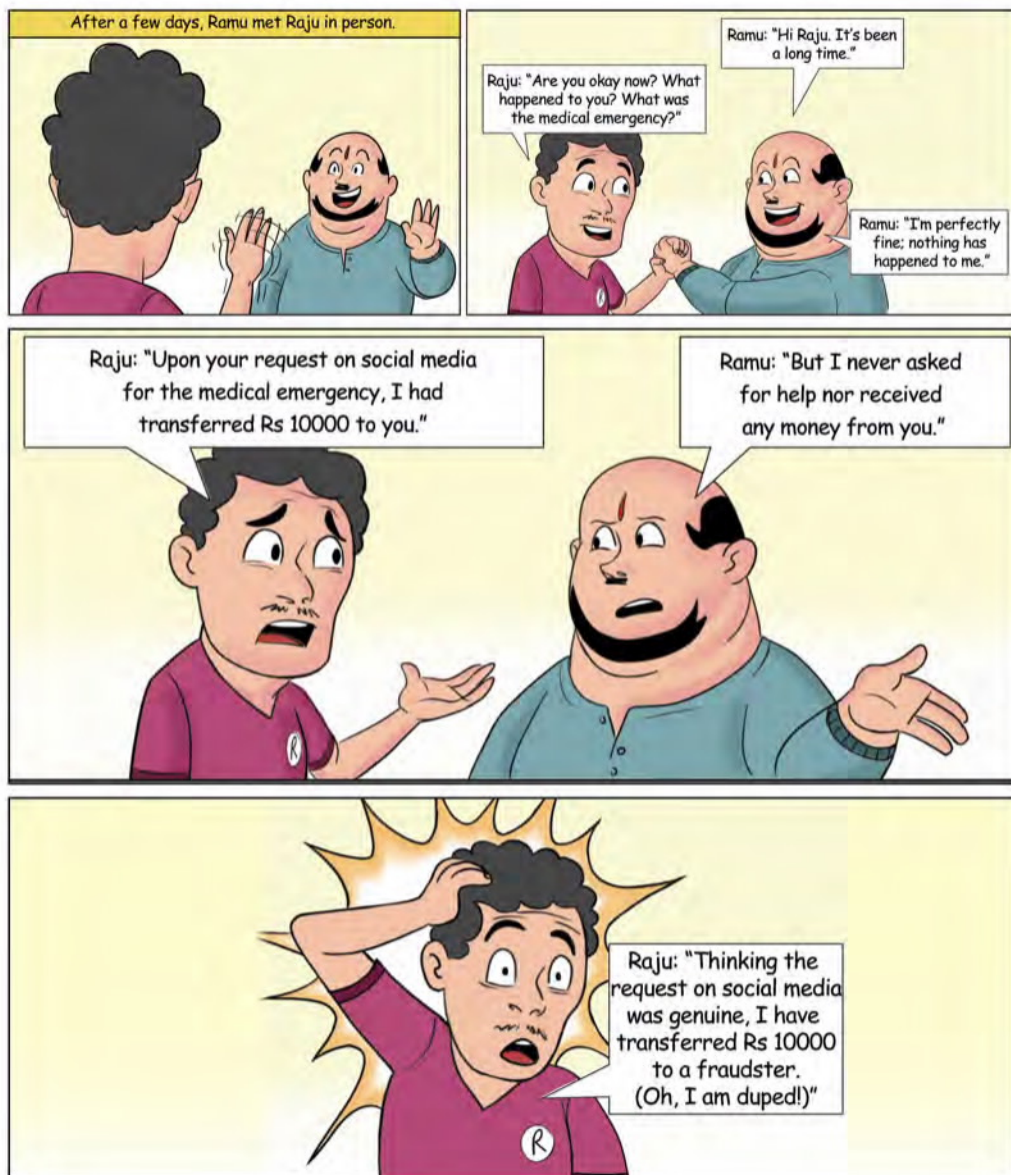


One day, Raju's friend, Ramu messaged him on social media requesting Rs 10,000 for a medical emergency. Raju immediately made the payment to Ramu using the shared account details.



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.

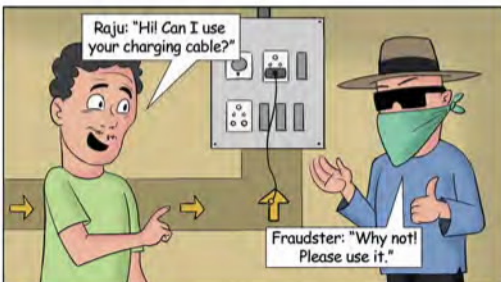
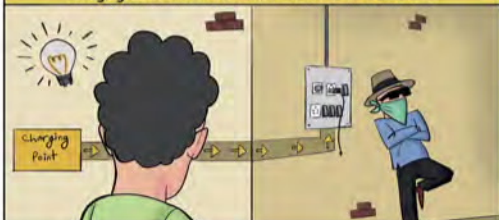
11. JUICE JACKING – STEALING OF DATA THROUGH CHARGING CABLE

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



Raju: "Oh no! My battery got drained, and I don't have a charger."

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.

Without thinking twice, Raju makes the payment.



Raju: "I have made the payment."

Fraudster: "Thank you, Sir! You will receive your prize within two days."

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



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

Don'ts:

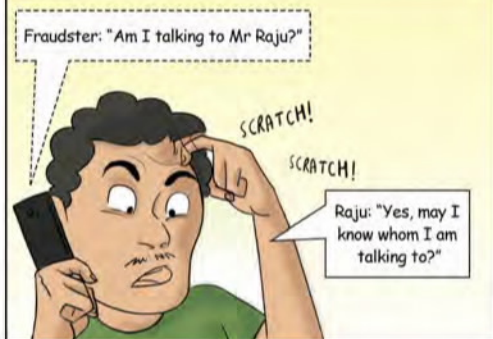
- × Do not make payments without verification, expecting very high returns.

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.

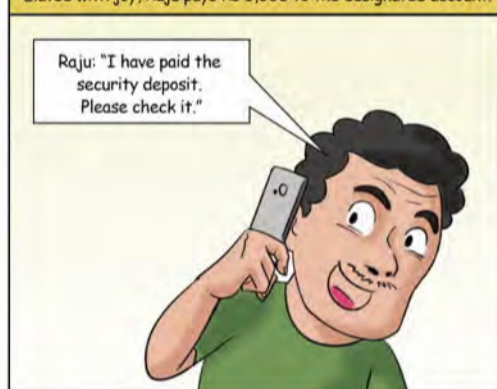


Do's:

- ✓ 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>



Elated with joy, Raju pays Rs 5,000 to the designated account.

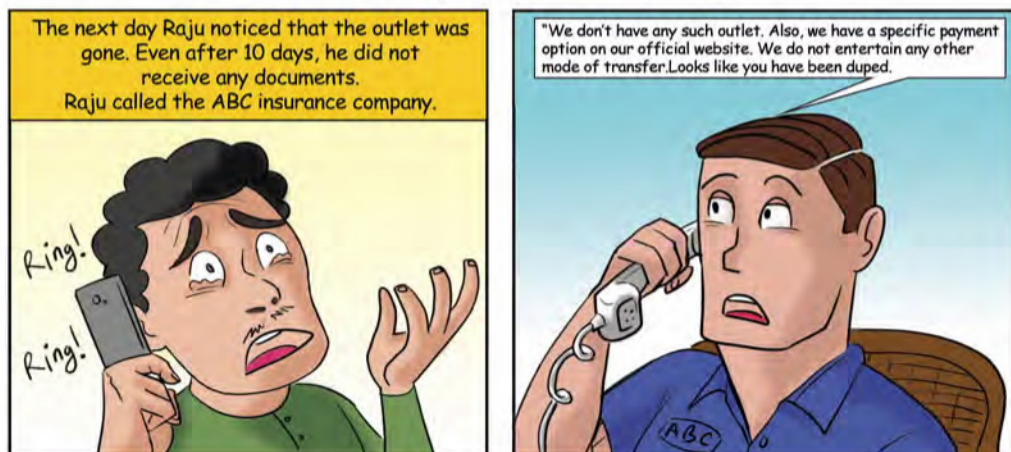


Despite waiting for several days, Raju did not receive any laptop. He tried calling on the number, but the number was always switched off. He searched the company name online but did not find anything. Raju eventually realized that he was defrauded of his hard-earned money.



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

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.



Ramesh: "Hello Raju. I am fine. How are you?
 You've called me after a very long time."



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>

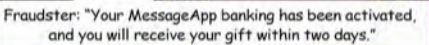
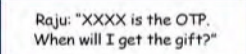
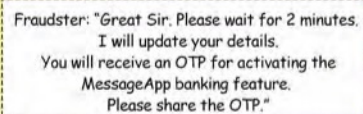


(Raju was in shock after knowing this. His act of kindness made him a victim to a fraudster due to his negligence. He should have verified the email ID.)

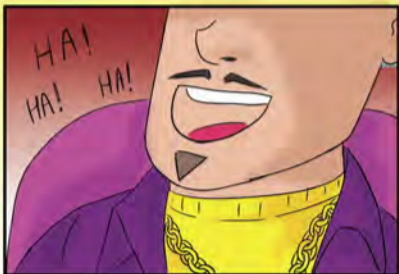


Don'ts:

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



Raju notices a debit message of Rs 20000 in his account. He immediately calls back, but the phone is switched off. Raju realizes that he has been duped.

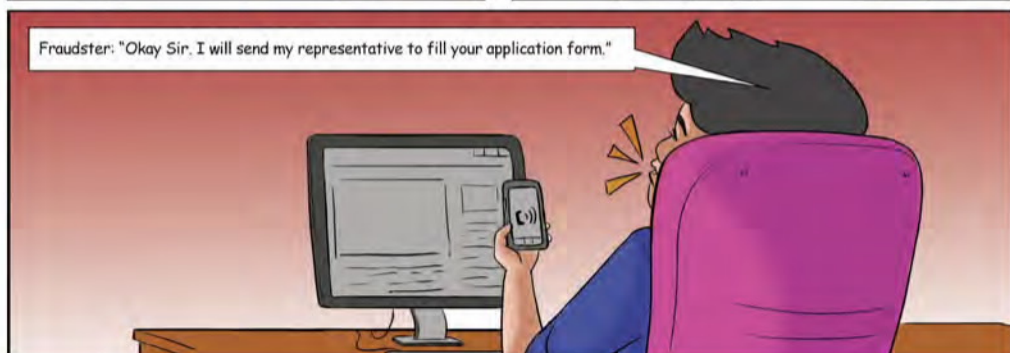
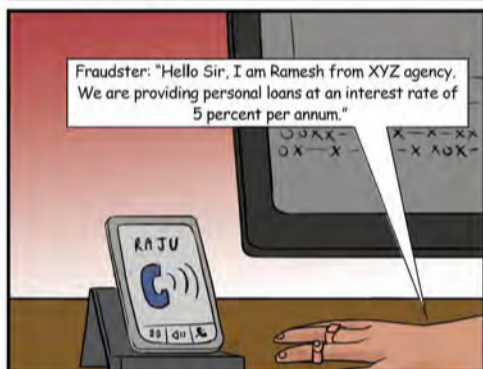
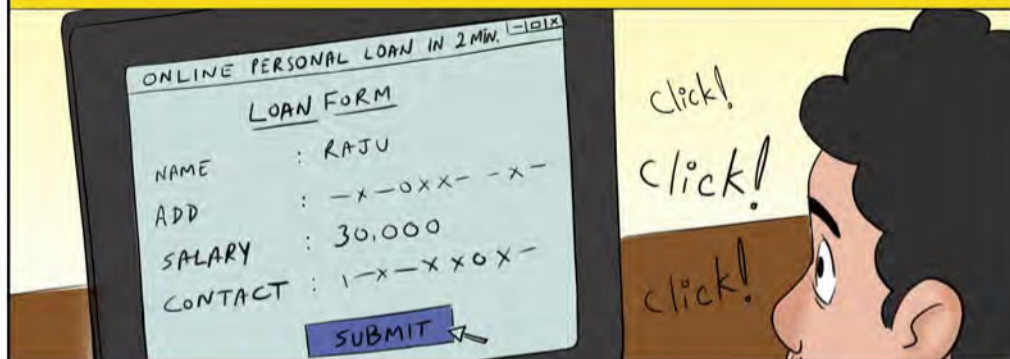


Don'ts:

- ✗ 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

Raju fills up several forms on the internet for availing of a personal loan.



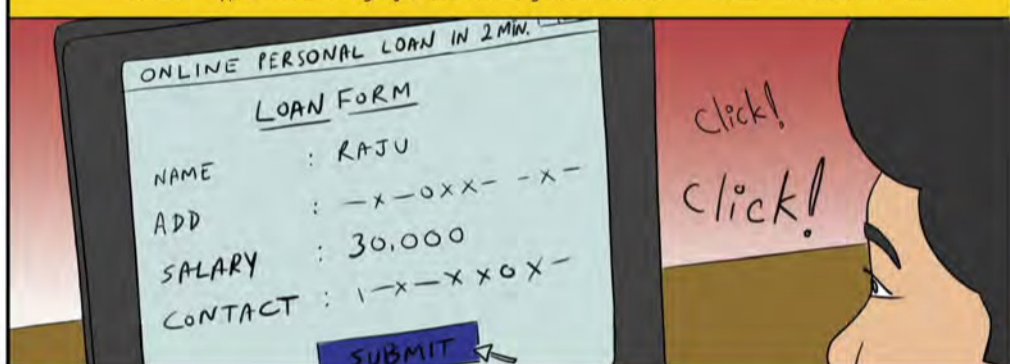
Do's:

- ✓ 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>

Raju fills the loan application form with all his details and provides a cancelled cheque to the representative.



The fraudster applies for a loan using Raju's documents but gives his own account number for the disbursement of the loan.



Raju: After a month, Raju receives a letter informing him Rs 10,000/- is due for the loan...

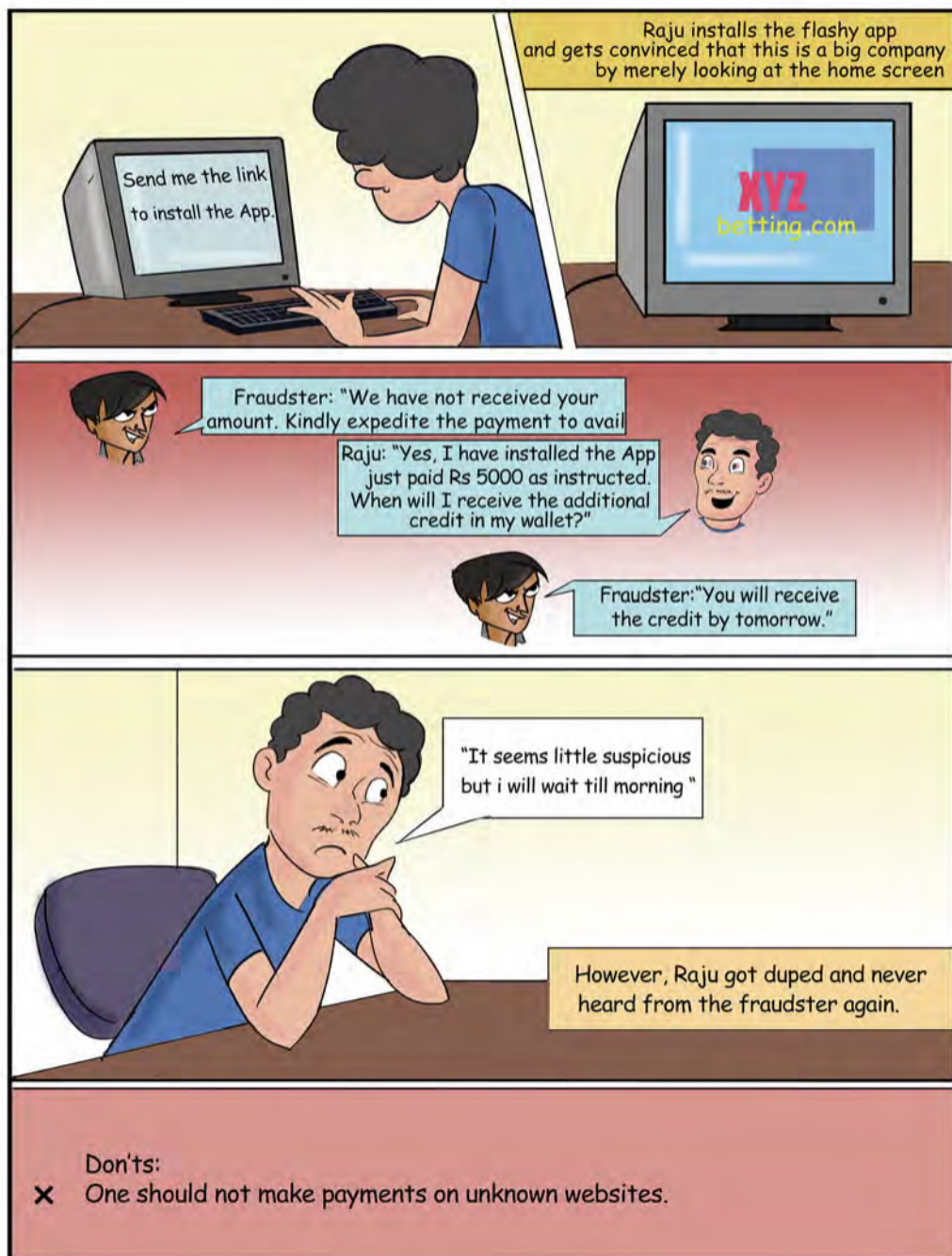


...Shocked, Raju calls the bank to inform them that he did not take any loan. But the bank shows the loan application form filled by him.



Don'ts:

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



19. FAKE VACCINATION CALL

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

"I am calling from the Local health Centre. We are calling to provide the vaccination facility at your home."



"Oh! Okay. But we can do it through the COWIN App only, right?"



"Yes Sir, but the home vaccination facility is not available on the App."



"Are there any extra charges?"

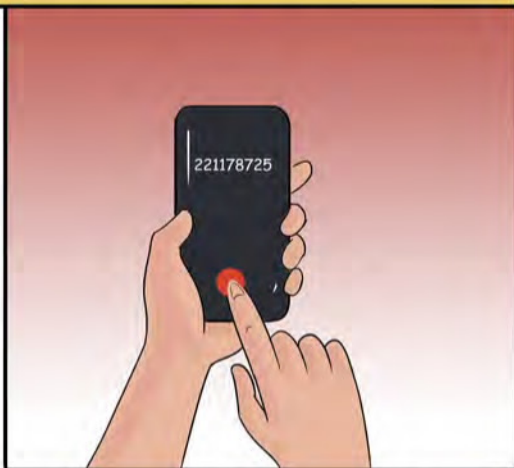
"No Sir, it is free of cost. I will verify your address and you will get registered for the vaccine. Please tell me your Aadhaar and PAN card details."



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.



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.



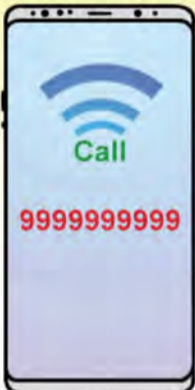
Don'ts:

- × 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.



22. SOCIAL WELFARE SCHEME FRAUD

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



"I am calling from the agriculture department. Your account details have not been updated for the KISAN scheme, hence your subsidy funds around 12000 Rupees are lying unused with us."



"What should I do to update the account?"

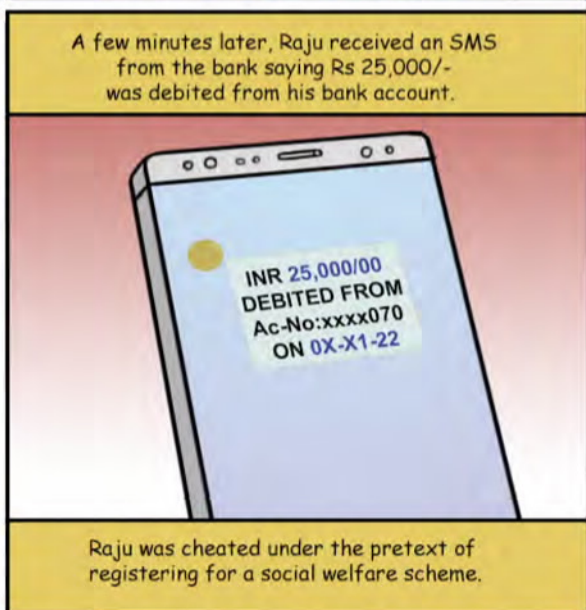


"You can visit the website and update on your own, or else, I will update it if you provide me your details."



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.

"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:
X Do not pay money to unknown companies and enrol in unknown schemes.

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.

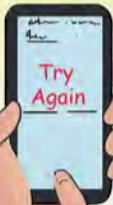
"Your total bill is Rs 12000, Sir. How would you like to pay, card or cash?"

RECEPTION

"I will pay online."

Raju initiated the payment but there was a network issue.

"I am facing connectivity issues during the transaction. Can you help me with this?"



"Sir, you can connect to the free Wi-Fi if your network is not working."

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

Poster:

**DIWALI BUMPER OFFER -
 THREE BRANDED
 WATCHES WORTH RS
 2500/- FREE FOR EVERY
 SINGLE WATCH
 BOUGHT!! HURRY UP!
 LIMITED PERIOD OFFER!!**

Please call
 Ph: 90xxxxxxx99
 for more details!

"Wow!! This seems great!
 I can buy one watch
 and get 3 free! Anyways,
 I wanted to give gifts to
 my cousins this Diwali holiday
 when I go home! I'd
 better call before the offer ends."



"Hi. I came across your
 Branded watch offer.
 Where is your location?
 I can come down to your
 store for the purchase."



"Sir! You are lucky.
 We are about to close the offer.
 You need not come here,
 Sir. We will deliver you
 the product at your address."



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>.

"That's great! Please send me pictures of the watches."



"Sure, Sir. I have shared them already.
I have also shared account details for transferring the amount. You must pay Rs 3000 to confirm the order. Once payment is successful, we will deliver the watches within 3 days. Hurry up, Sir. The offer ends in another 30 minutes. Happy Diwali!!"



"Okay. I have shared my address. I'll send the money right away."



"Oh no! Why haven't they delivered yet!!? Their phones are switched off..How do I trace them now!!? I think I have lost the money!"

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."



"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."



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



"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>.

"Sir, this offer is valid only for today. You need to send a processing fee of Rs 5000 immediately to avail of this offer. I have shared the account details for transferring the fee."



"Oh! Is that so? Then I'll send the processing fee now. I will also send the rest of the details to your number soon."



Raju makes the payment. However, even after weeks, he does not receive any response from the company, and the number from which he received the call no longer exists.

"Okay, Sir!! We will update you on the loan application within a week! Thank you."



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

Another day, Raju received a call from the bank.

Hello, Mr Raju.
I am calling from XYZ Bank.
Congratulations, Sir.
Your credit card is
eligible for a limit upgrade."



"Oh, thanks.
What will be the new limit?"



"The new limit will be
increased to Rs 5 lakh
from your current limit
of Rs 1 lakh."



"Oh, that's great!"



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>.



"Sir, you'll need to confirm the free limit upgrade code which will be delivered to you. Shall I proceed?"

"Yes, please."

"Your card number is 4500 1000 1000 1000. You must have received an activation code in SMS. Please share."

"Yes, it's 123456."

"OTP for txn is 123456"

"Thanks for the confirmation. Your card limit is upgraded now, and you will receive an SMS regarding this within the next 2 hours. Have a nice day!"

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.

"Hello Sir! I am calling from ABC.com.
 Sir, we are glad to inform you that we are providing you with a 50% cashback on your recent purchase from ABC.com."



"Oh really. 50% cashback is huge. Thank you so much...!"



"You are our valuable customer, Sir."



"Okay, so tell me. When will the cashback be credited to my account?"



"It won't take much time, Sir. You need to open the app, and there will be a pop-up message regarding the cashback."



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>.

"I've opened my app now. It is showing a payment request of Rs 20,000/- to abc.com"



"That is correct, Sir. We must take your approval to credit cashback in your account. So please click on Pay."



"Okay, now it is asking for my UPI PIN."



"Please enter your PIN as it is just for verification purposes."



"Okay."



"Thank you, Sir. You will shortly receive credit in your account."



(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.

**NEWS
REPORT**

Actor Monu gifts 100
smartphones to Government
school students

Raju searched on the
internet about the
actor's charity
foundation
and called up the
number.

MONU
charity
Foundation

"Hello, Sir. Is this actor
Monu's charity foundation??"

"Hi Sir. This is his
office's number.
I am his personal
secretary.
How may I help you?"

Do's-

- ✓ Always cross-check charity organizations' credentials on the Government 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>



"Sir. I am Raju, calling from xxxx government school. I saw the news of your charity to the students. Sir, we have 100 poor students in our school who cannot afford laptops / smartphones. Can you please help us, Sir?"



"That would be great! Sir."



"Okay, Sir. I'll send you the registration fee right away. Please share your account details."



"Oh yes! Thank you so much for reaching out to us on behalf of poor children. I assure you of help."



"Okay. Please share your address. We will send you 100 smartphones. However, you will have to pay a token registration charge of Rs 50,000/- today itself for us to send the phones. The phones will be delivered in a week, and we will refund the registration fee after delivery."



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.

"Hi, I received an SMS regarding freelance work. What is the work profile?"



(This is very easy, even my kid can do it.)
 "Okay, I am interested."



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.

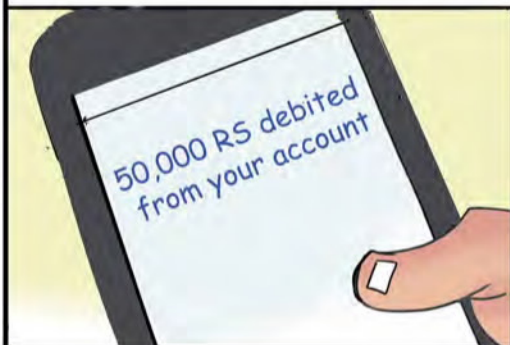


Over time, the fraudster was able to get all the secure credentials from Raju's device through his application. Unaware of the malafide intention, Raju continues to use the application. The fraudster was also able to get the OTP sent on Raju's email since the fraudster got access to his email.

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.

Within 7 days, Raju started receiving calls for repayment of Rs 7500/- . Raju still had not arranged money to repay the old loan and gets shocked by the demand of Rs 7500/- as repayment for the Rs 5000/- loan. Raju approached another friend, Laxman.



"I was under the impression that I will repay my loan amount along with nominal interest charges, but this app is charging exorbitant interest and many other charges. What shall I do now?"



Oh! Did you verify whether the entity is registered with RBI or have any other valid registration? Else, they would not be covered under any rules, and you are bound to pay as per the agreement only. Always check whether the finance company (NBFC) is registered / licensed by RBI

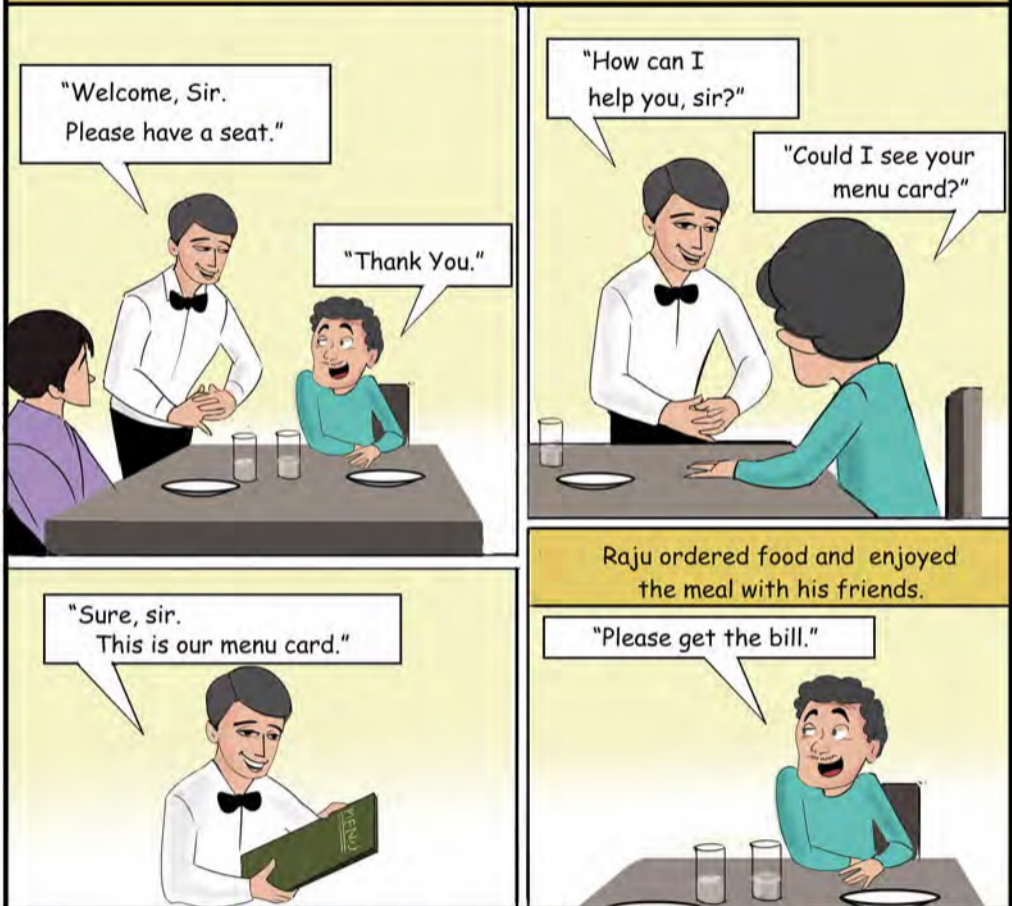


Don'ts:

- ✗ 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.

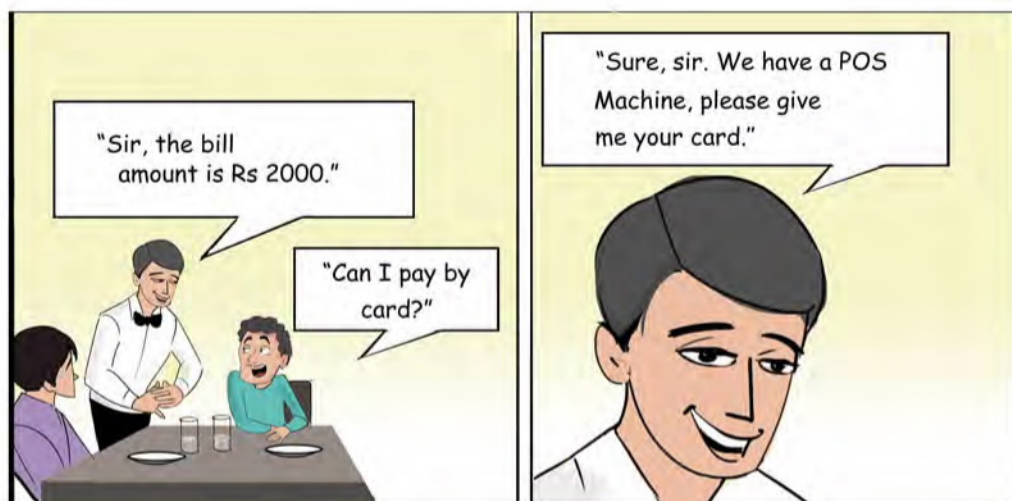
38. CARD CLONING AT MERCHANT OUTLETS

One day, Raju went to a restaurant along with his friend for lunch. He called the waiter.

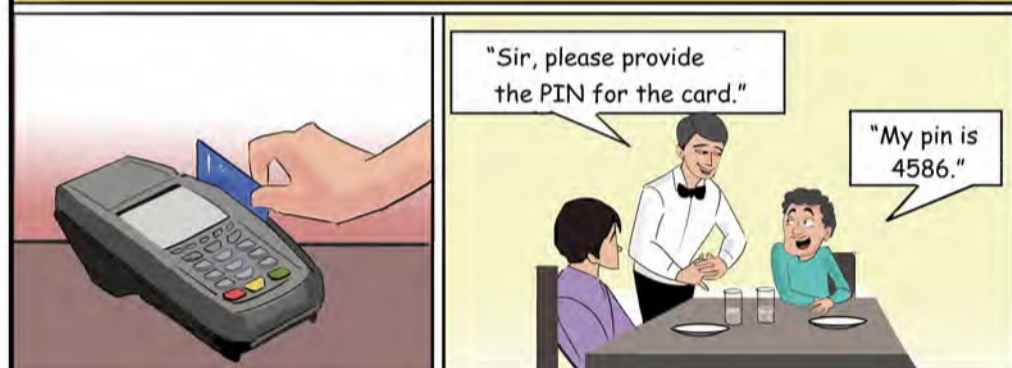


Do's:

- ✓ 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**