

# Raju & The Forty Thieves



## *A Booklet on Modus Operandi of Financial Fraudsters*

Consumer Education and Protection  
Department (CEPD), RBI

<https://cms.rbi.org.in/>





## Foreword

With the Indian financial system caught up in the throes of a technological and digital revolution, the Reserve Bank of India (the Bank) recognizes the felt need to further 'preventive financial awareness' amongst common public, especially for the newly initiated into the digital financial world, who may not be well-versed with the nuances of online fraudulent transactions and thus be vulnerable to digital frauds. As part of its customer awareness initiatives, in March 2022, the Bank released a booklet 'Be(A)ware' on the common modus operandi used by fraudsters and precautions to be taken while carrying out various financial transactions. The booklet received positive response from members of the public and other stakeholders.

Extending the concept of Be(A)ware over to a pictorial mode, another booklet, namely, 'Raju and the Forty Thieves' is released to create awareness among the public and customers, across all age groups with different education levels, including, inter alia, school children, young adults, semi-literates and senior citizens, etc., irrespective of their place of habitation. The booklet is a lucid pictorial depiction of the modus operandi observed in fraudulent financial incidents and aims to help learn from common mistakes and take steps to protect themselves and their hard earned money from fraudsters.

As the name suggests, 'Raju and the Forty Thieves' covers forty stories providing glimpses of fraudulent acts reported to the Bank, including the RBI Ombudsmen and the Consumer Education and Protection Department (CEPD) and provides simple tips about Do's and Don'ts as safeguards against such incidents. Raju is a typical gullible citizen, and, in these stories, he appears in different characters/roles, be it that of a senior citizen, a farmer or a happy-go-lucky individual, etc., to enable different stakeholders identify themselves with him in different walks of life.

The creative efforts put by the team of RBI Ombudsman, Mumbai – II, Maharashtra and Goa in preparation of this booklet is gratefully acknowledged.

We urge the readers to make themselves aware of the modus operandi used by fraudsters and further spread this awareness by educating those around us. Readers are encouraged to share their feedback/suggestions with us at [cgmcepd@rbi.org.in](mailto:cgmcepd@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



<b>SL. No.</b>	<b>Topic Name</b>	<b>Page Number</b>
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 a 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: "Oh! All my money will be blocked; I need to update my KYC details."

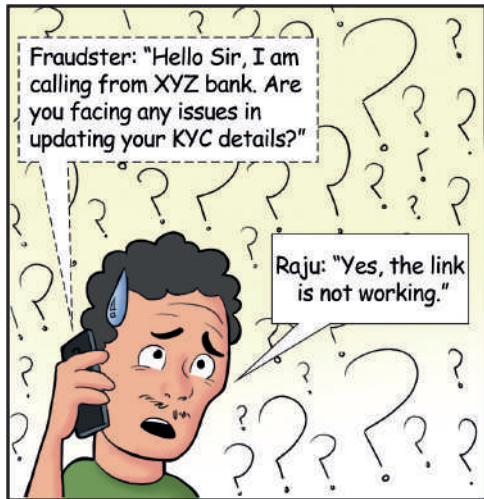


Raju clicked on the link, but the link to update KYC details did not work. Soon, he gets a call.



Fraudster: "Hello Sir, I am calling from XYZ bank. Are you facing any issues in updating your KYC details?"

Raju: "Yes, the link is not working."



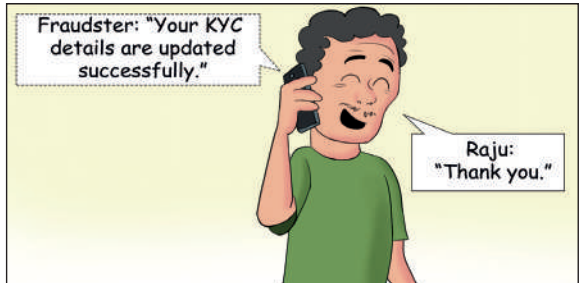
Fraudster: "The website load might be high; I will update the details manually. Please share your username, password and OTP."

click!  
click!

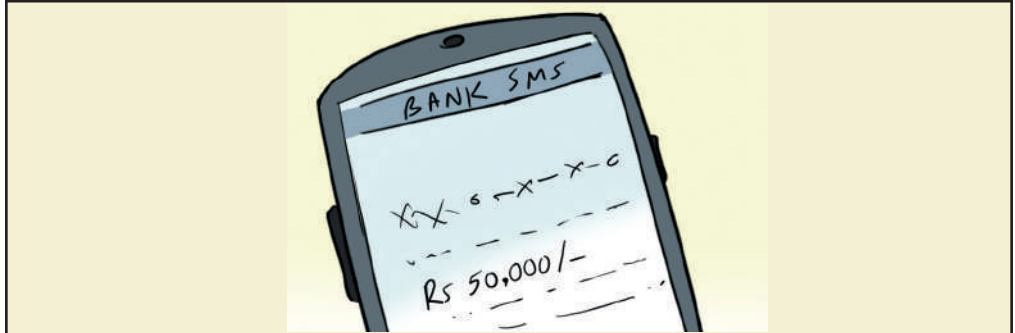


### Do's:

- ✓ 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

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 Rs. 18000/- 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."

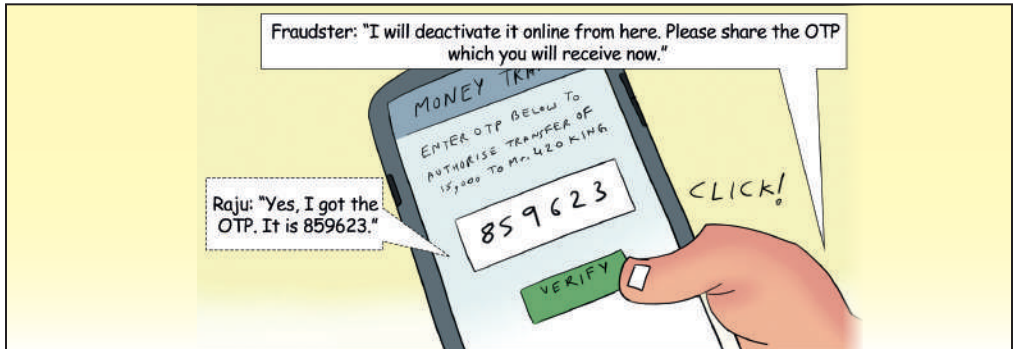
Raju: "I don't understand how you activated the policy without my consent, and why should I trust you?"

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>



- 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 a sofa set. He posted an advertisement on a 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 the 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."

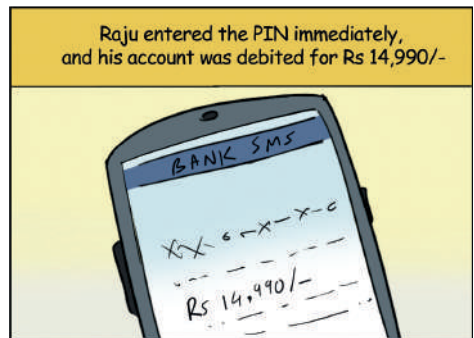
The fraudster sent Rs. 10/- to Raju's account and asked for confirmation to initiate the final payment.

Raju: "Okay, I got it."

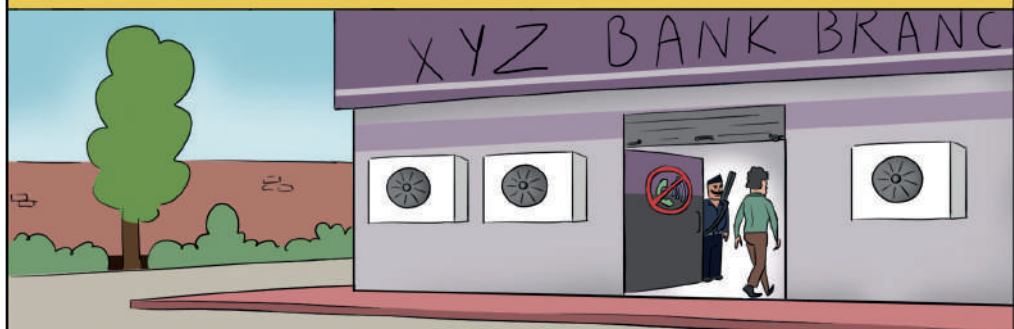
**Do's:**

- ✓ 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 approached 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 payment from another person.




## 4. CREDIT CARD ANNUAL FEE WAIVER- FAKE OFFER

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



Fraudster: "Good morning, Mr Raju! I am Rohit Kumar from your Bank customer care. We are happy to inform you that your credit card annual fee will be waived for this year as you are one of our most valuable customers."

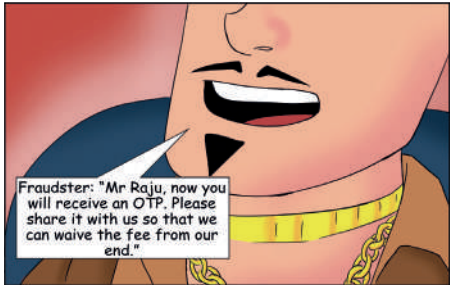
Raju: "Oh! That's great news."



Fraudster: "Mr Raju, Please confirm a few details before I can proceed further. Your card number is 42781234 XXXX, and your full name is Raju Deshpande, right?"

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

Raju: "Yes, these are correct."



Fraudster: "Mr Raju, now you will receive an OTP. Please share it with us so that we can waive the fee from our end."

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.

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



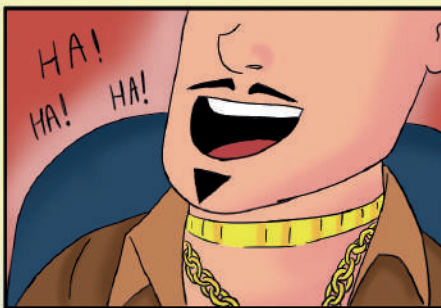
The call was disconnected. Soon, Raju received an SMS stating that Rs. 12,000/- was debited from his credit card account.



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

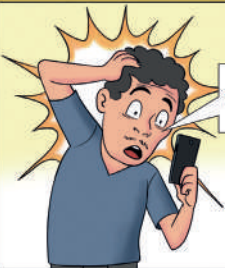
Raju receives his monthly salary in his account. He visits an ATM to withdraw money for his monthly expenses.



click!  
click!  
click!

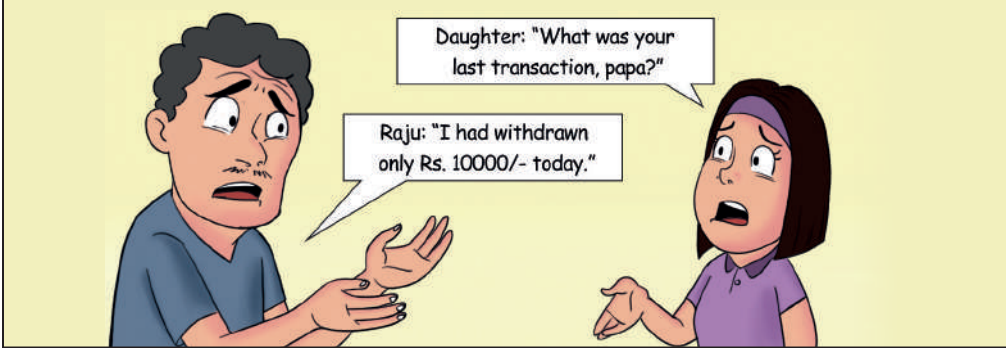
Raju withdraws the money, and he gets an SMS alert for his transaction.

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 Rs. 10000/- 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?"

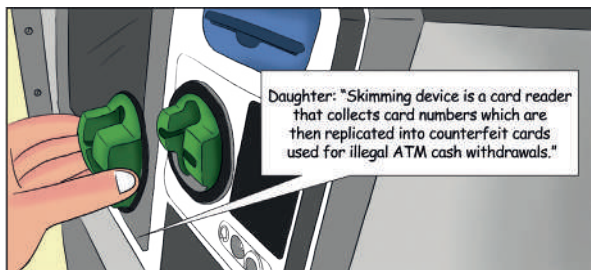
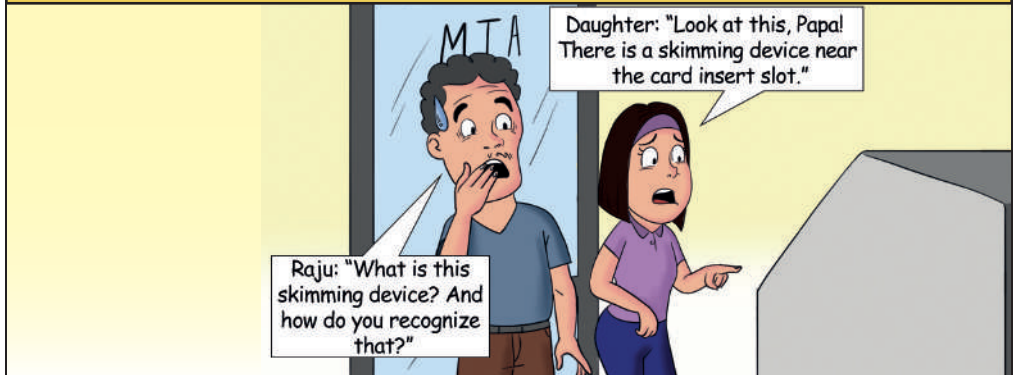


TAP!  
TAP!  
TAP!

- 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 fraudulent 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.



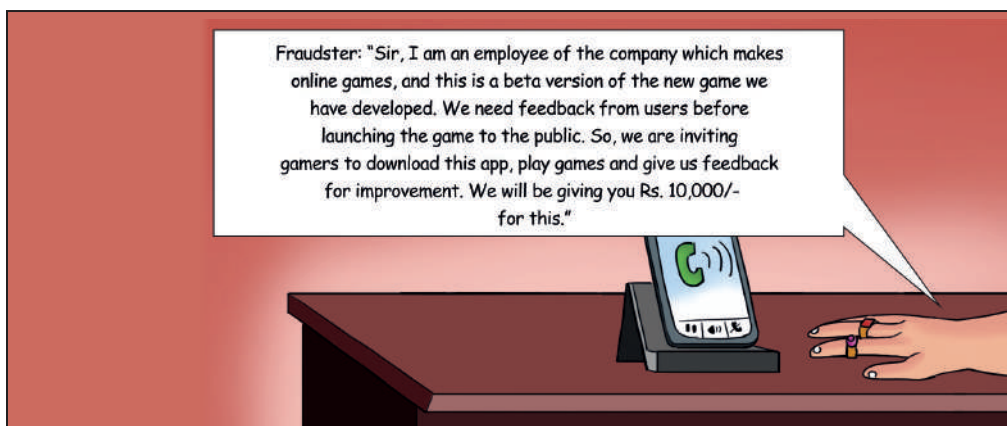
**Don'ts:**

- × 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.



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

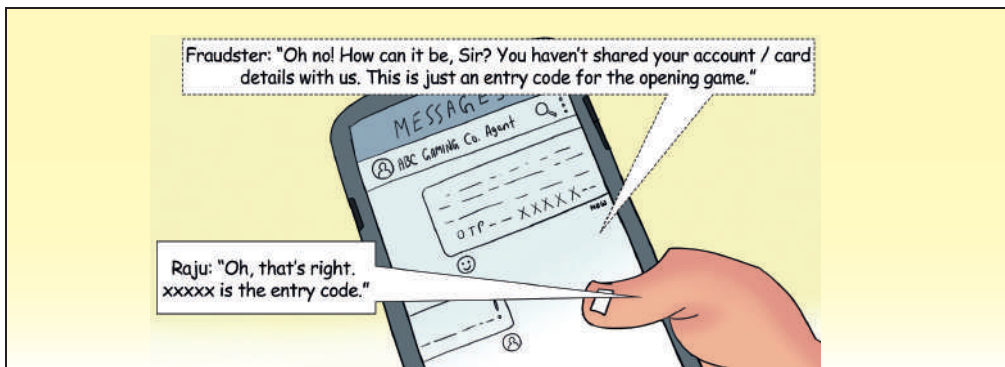


Fraudster: "Sir, you will see a code for logging into the app. Please share it with us."

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

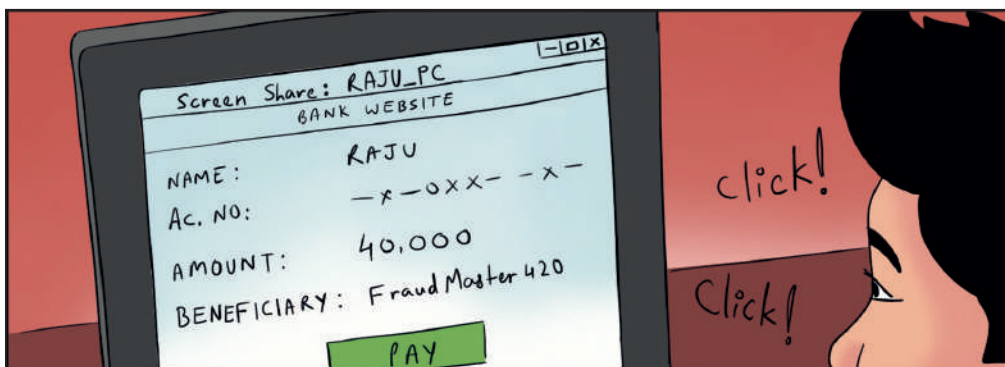
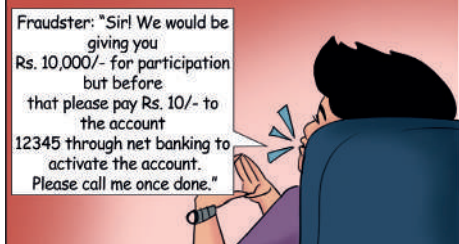
### Do's:

- ✓ 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.

Raju thinking that it was just a matter of Rs. 10/- transferred the amount through Net Banking. Soon he received debit messages of Rs. 35,000/-, Rs. 20,000/- and Rs. 40,000/-.



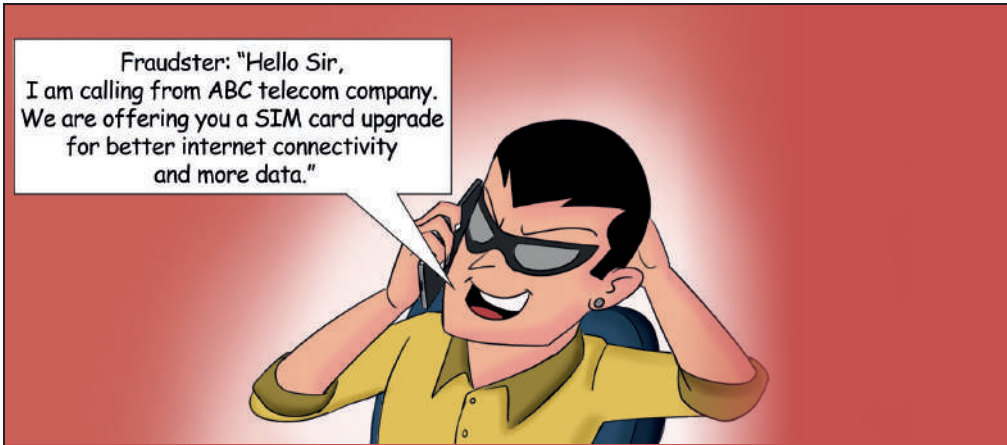
Once the screen-sharing application was installed, the fraudster had access to the net banking password entered by Raju for making the payment (of Rs. 10/-).

**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 such as : forgot username, reset password etc. and transfers 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.

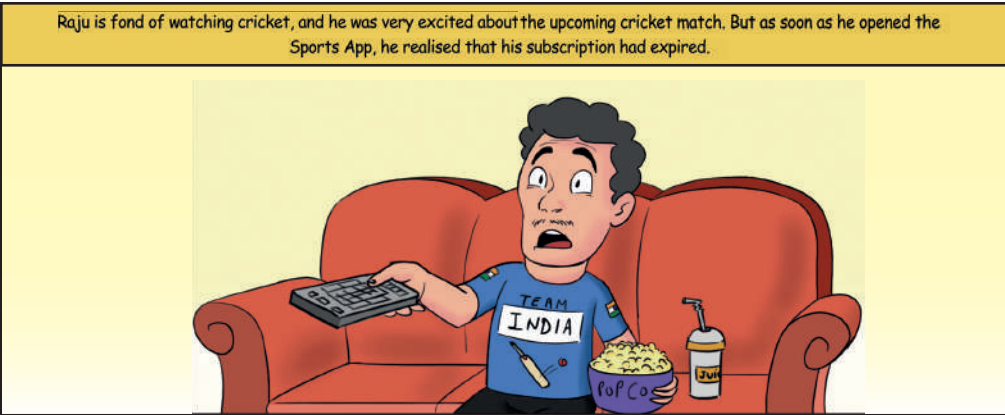


**Don'ts:**

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

## 8. FRAUDS BY COMPROMISING CREDENTIALS THROUGH SEARCH ENGINES

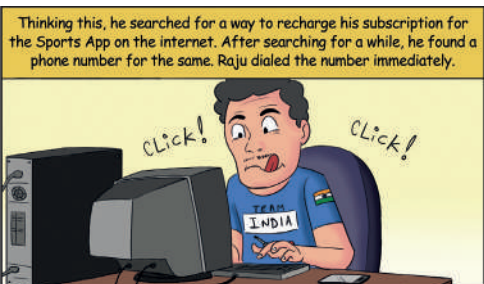
Raju is fond of watching cricket, and he was very excited about the upcoming cricket match. But as soon as he opened the Sports App, he realised that his subscription had expired.



Raju thinks: "What is the big deal  
The Internet has all the solutions."

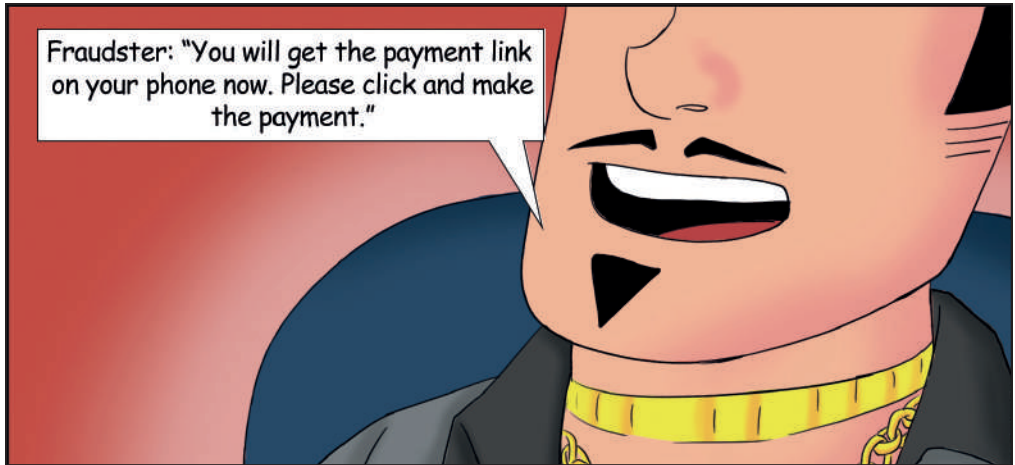


Thinking this, he searched for a way to recharge his subscription for the Sports App on the internet. After searching for a while, he found a phone number for the same. Raju dialed the number immediately.



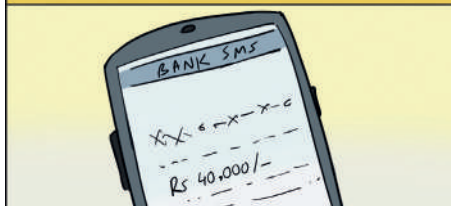
### Do's:

- ✓ 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>

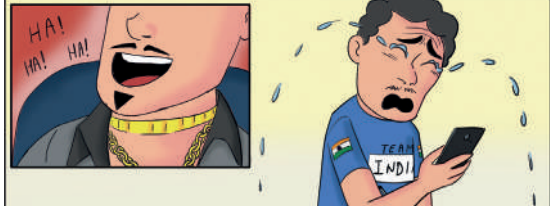


Raju clicked on the link, entered the OTP and made the payment without verifying the amount.

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 transactions.

## 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."

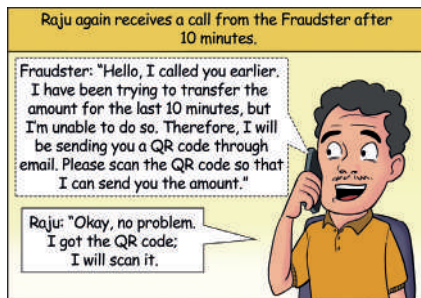
Raju: "That's great! I guess you want to check the car before buying it."

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."

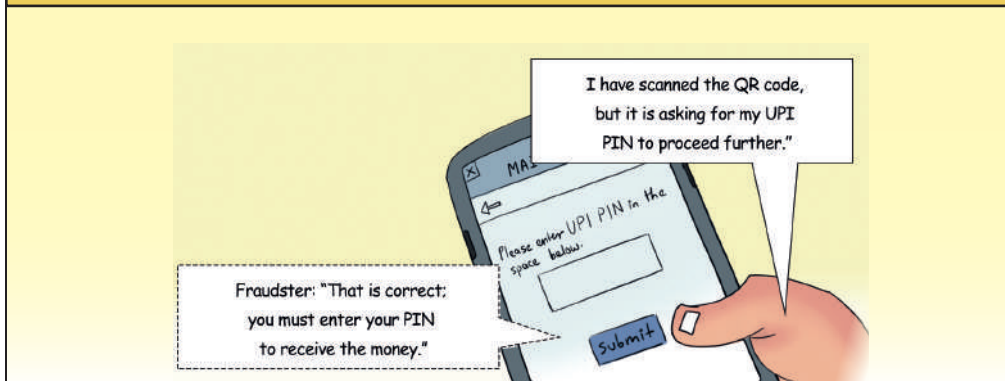


### Do's:

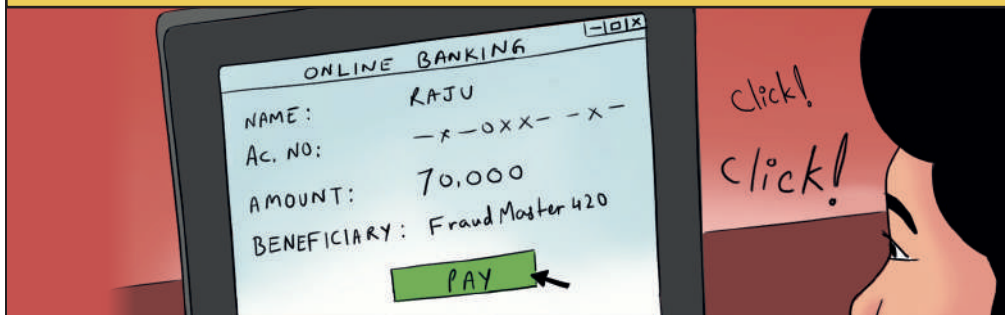
- ✓ Educate yourself about QR codes before using them.
- ✓ Report the transaction immediately to your bank.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



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

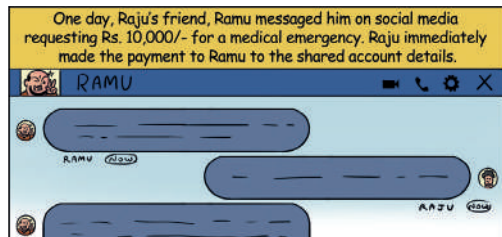


Raju believed him and entered his UPI PIN. Subsequently, his account got debited with Rs. 70,000/-. Raju received an SMS alert of the debit. He panicked, so he tried calling the fraudster, but his phone was switched off by then.

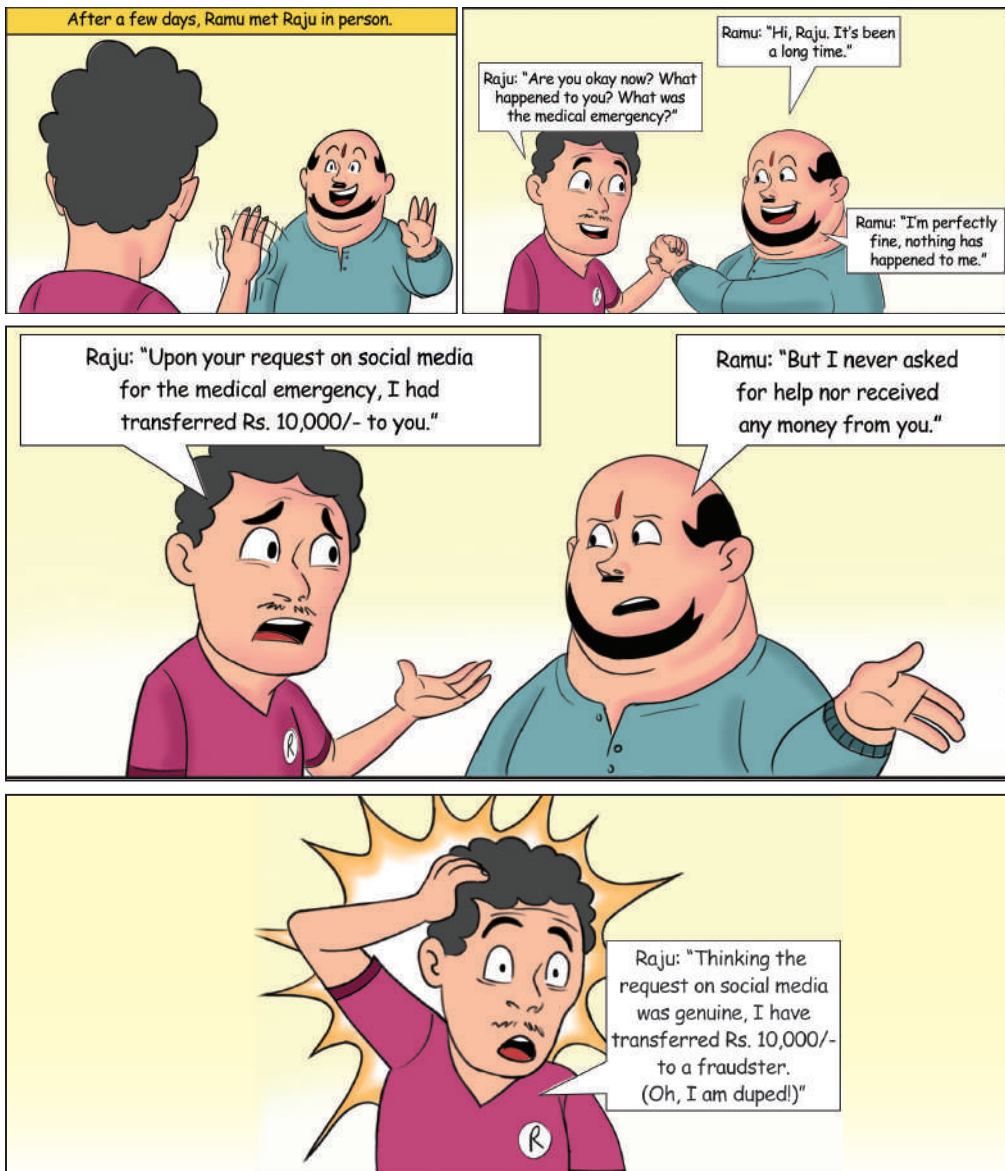


- Don'ts:**
- × Don't enter your UPI PIN to receive money from another person. UPI PIN is required only while making a payment, not for receiving money.
  - × Don't scan QR codes to receive any payment. QR code needs to be scanned for sending a payment, not for receiving Money.

## 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>

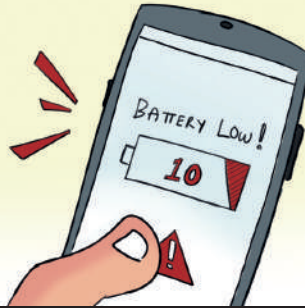


**Don'ts:**

- × 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.

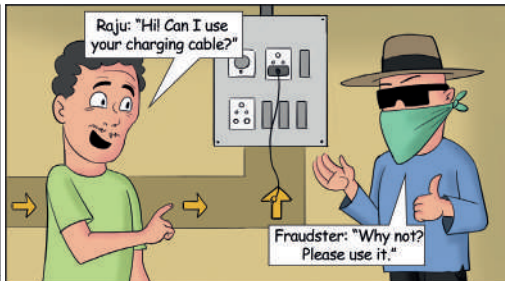
## 11. JUICE JACKING – STEALING OF DATA THROUGH CHARGING CABLE

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



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.



Raju: "Hi! Can I use  
your charging cable?"

Fraudster: "Why not?  
Please use it."

### Do's

- ✓ Install anti-virus software on your mobile phone to protect it from any 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 offered or provided by strangers in public places.

## 12. LOTTERY FRAUD

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



Fraudster: "Hi... I'm Pankaj calling from ABC. Congratulations on winning the ABC jackpot of Rupees 10 Lakh. I have sent you the jackpot details. You may contact the number mentioned therein to claim the prize. Hurry up!"

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.

Raju: "Hi, this is Raju. I was asked to contact you for claiming the ABC Jackpot. How shall I claim my jackpot?"



Fraudster: "Congrats Rajul You must pay a delivery fee of Rs. 1,000/- to be eligible to receive the prize. I have shared our account details on your Message App number. Please pay the amount immediately and call me back."



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

Raju: "Hi, I have paid the amount and sent you the details. When will I get my prize?"

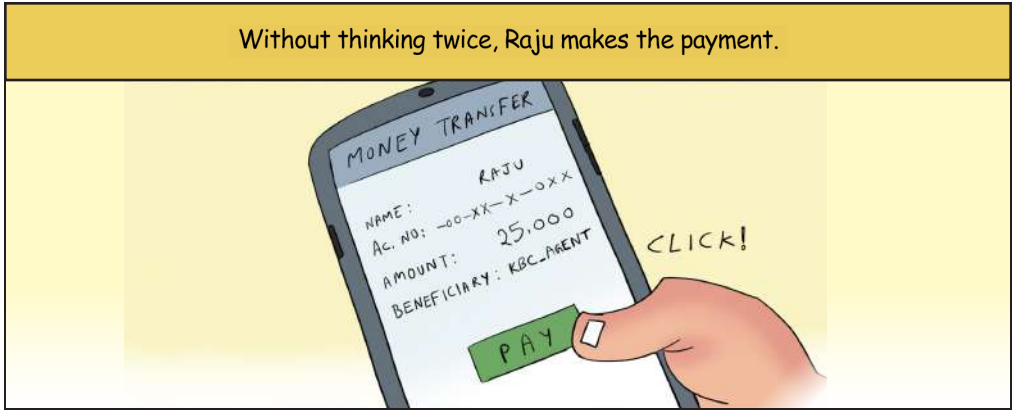


Fraudster: "Excellent Rajul We have only a few more steps to complete before you get the jackpot of Rupees 10 lakh. You will have to pay a tax fee of Rs. 25,000/- to claim the prize amount."

### 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.

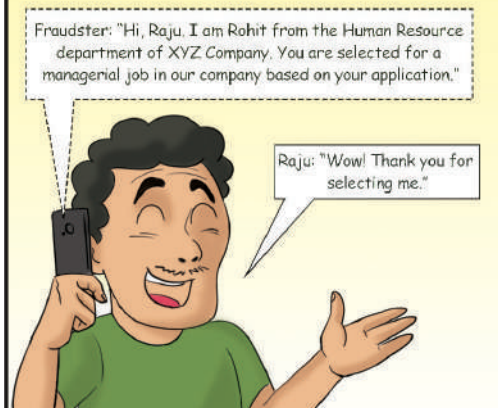
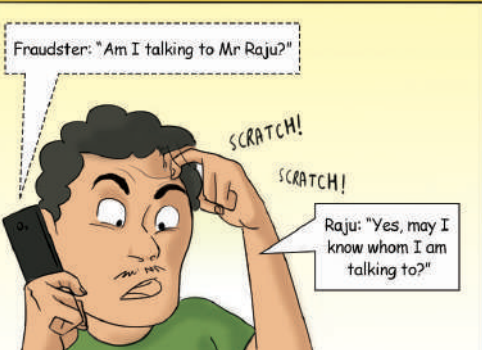
- Don'ts:
- × Do not make payments without verification, expecting very high returns.

## 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.

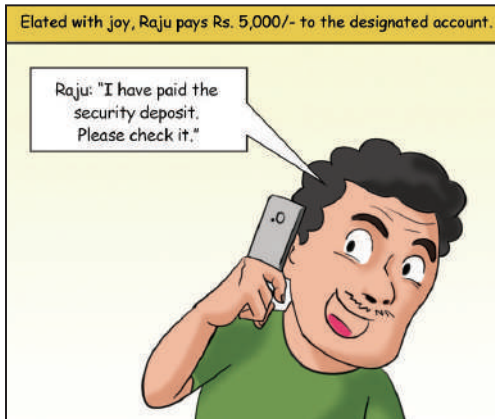


One day, he got a call from a fraudster, impersonating a person from XYZ Company.



### 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>

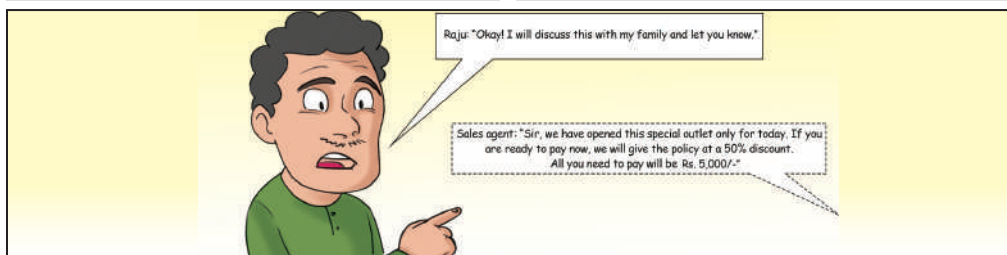
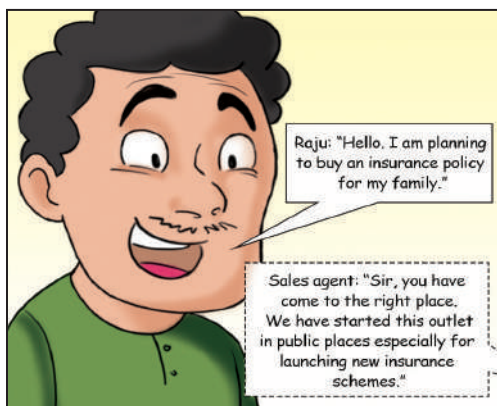
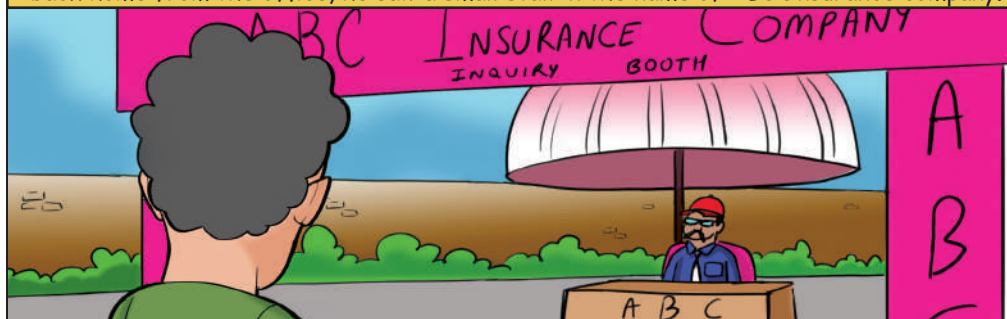


**Don'ts:**

- ✗ 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.

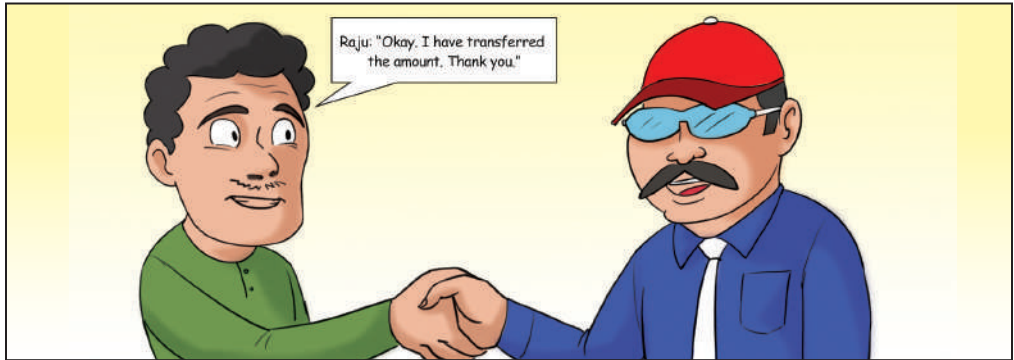
## 14. FAKE ACCOUNT NUMBER

Raju was planning to buy a family insurance policy for himself and his family. On his way back home from the office, he saw a small stall in the name of ABC Insurance company.



### Do's

- ✓ Cross-check an organization's credentials on a known database to verify if they are genuine.
- ✓ Always approach the 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>



The next day Raju noticed that the outlet was gone. Even after 10 days, he did not receive any documents. Raju called the ABC insurance company.



"We don't have any such outlet. Also, we have a specific payment option on our official website. We do not entertain any other mode of transfer. Looks like you have been duped."



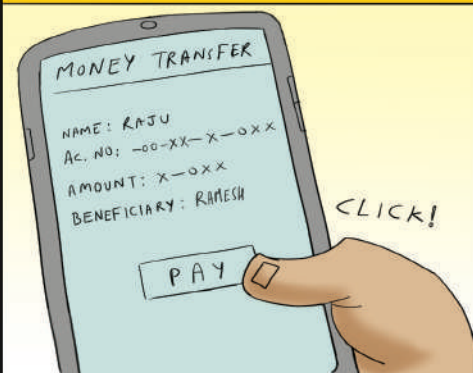
**Don'ts:**  
X Do not pay anybody without verifying the authenticity of the company.

## 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.

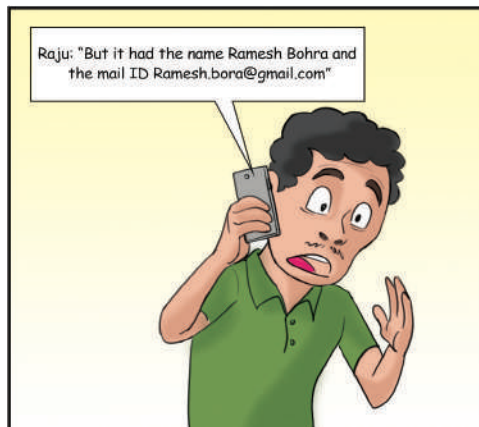


Ramesh: "Hello Raju, I am fine. How are you?  
You've called me after a very long time."



Do's:

- ✓ Verify with the person concerned before making any payment based on an 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>



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



**Don'ts:**  
X Don't make payments on receiving requests from random emails or similar-looking email ids.

## 16. MESSAGE APP BANKING FRAUD

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

Fraudster: "Hello, Sir. I am calling from the customer care centre of XYZ Bank. We are launching a new product on MessageApp. It's a banking facility that provides 24\*7 banking services easily through your MessageApp. You will also receive a gift voucher when you use it for the first time. Please confirm whether 99\*\*\*\*\*99 is the mobile number registered with MessageApp."

NAME: RAJU  
OCCUPATION: XOXO  
ADDRESS: X X - X X  
X X - X X O X - X - O X  
X X X X O X - X X  
CONTACT: 729256027  
X - X - X - X



Raju: "Wow! That's amazing. Yes. This is my MessageApp number."

Fraudster: "Okay Sir. We have already sent you a welcome message on MessageApp. Please check."

Raju opens his MessageApp and sees a welcome message from a number with the poster of XYZ Bank as its profile picture and the bank's tagline as its status.

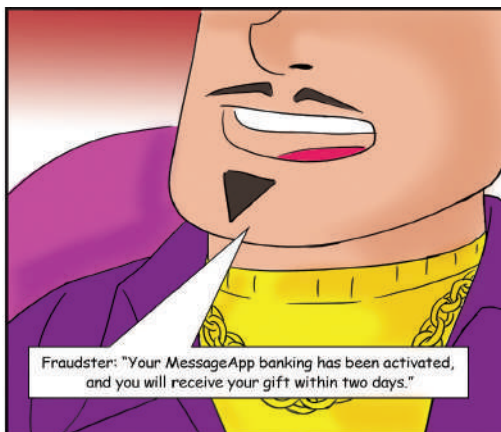


Fraudster: "Please enter the details of your debit card for verification. You do not have to share the details with me but enter it only on the official MessageApp number."

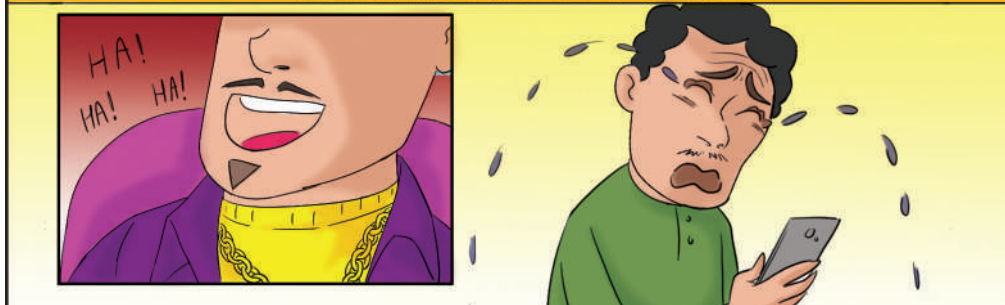
Raju: "I have entered it."

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>.



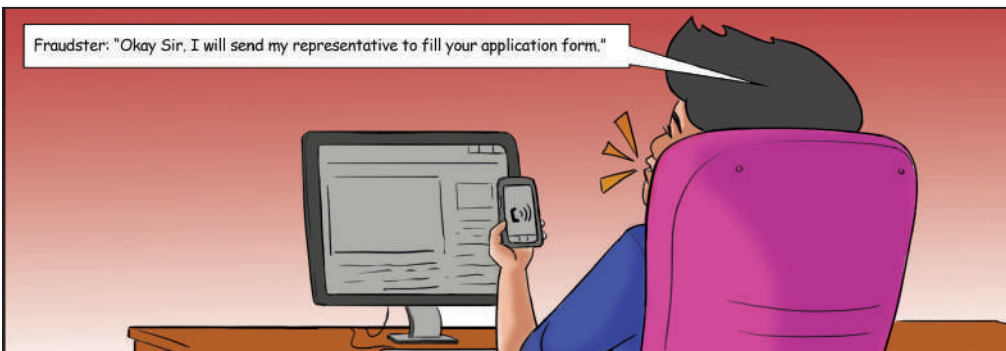
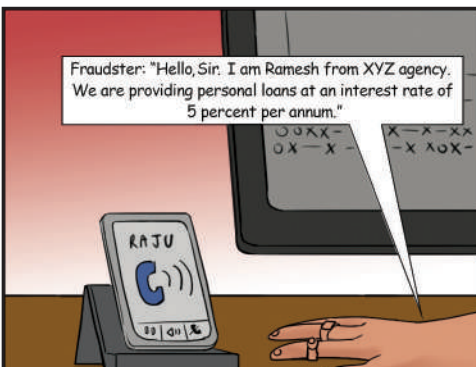
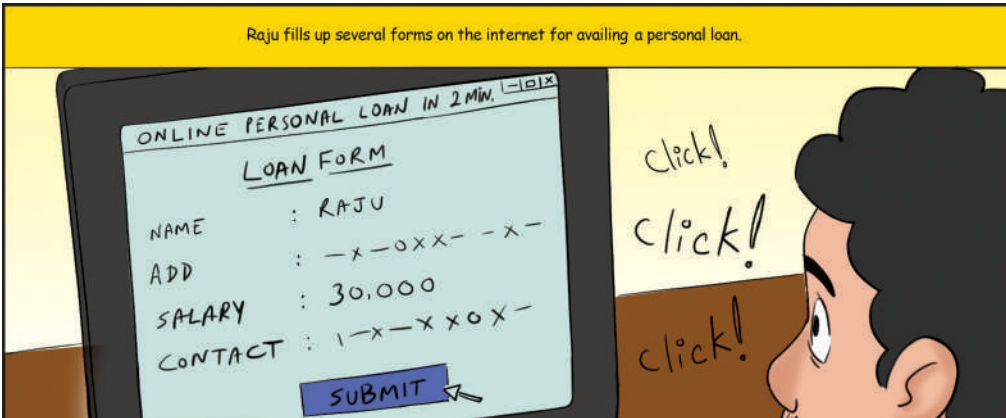
Raju notices a debit message of Rs. 20,000/- in his account. He immediately calls back, but the mobile is switched off. Raju realizes that he has been duped.



- Don'ts:
- × Don't trust unknown callers offering easy banking services and sending texts through Messaging Apps.
  - × Don't share card details and OTP with anyone.

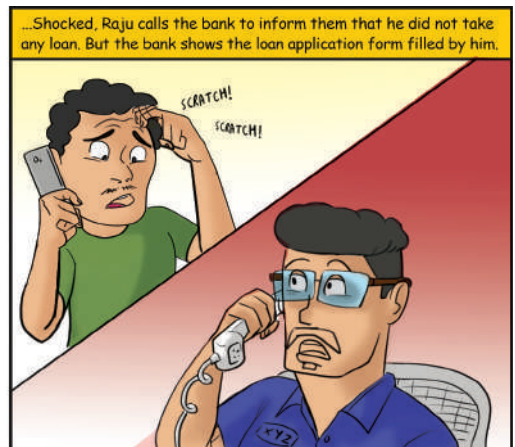
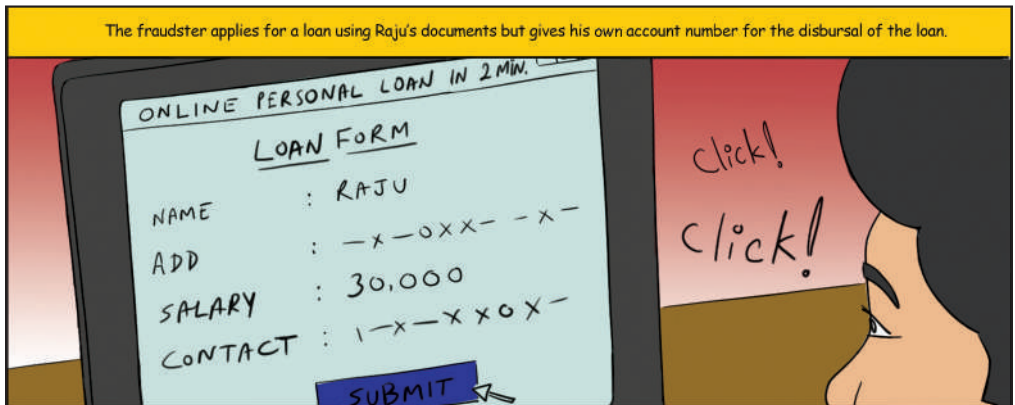
## 17. FRAUDULENT LOANS WITH STOLEN DOCUMENTS

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



### Do's:

- ✓ Always monitor the end-use of the documents when submitting them.
- ✓ 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

Raju was excited for the latest season of JKL cricket.

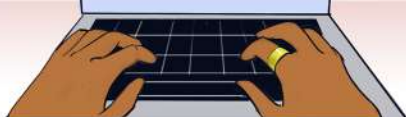
The new JKL cricket season is here. There are many stories of easy money through betting. I must try it.



Raju searches for JKL betting groups on the internet.



Welcome, Mr Raju. We are glad you enquired about the betting. How may I help you?"



"I want to place a bet for this JKL season."

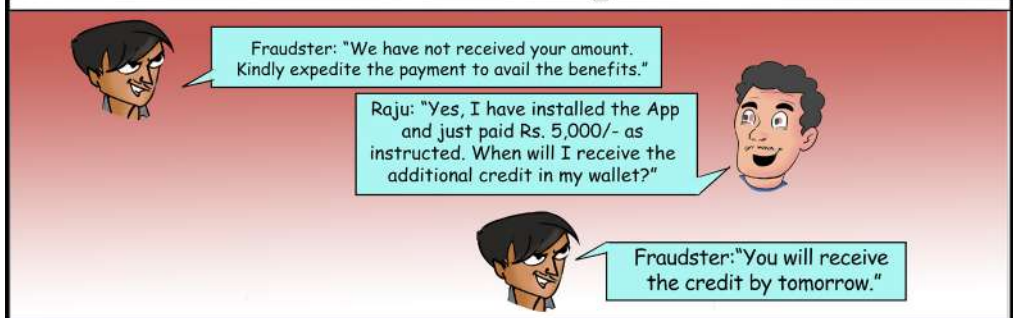


Fraudster: "First, you need to register on XYZ betting.com and as a welcome gift you will receive Rs. 5,000/- on your first recharge of a minimum of Rs. 5,000/-."



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>



- Don'ts:
- ✗ One should not make payments on unknown websites.

## 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 understand the purpose for which OTP is generated.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



"My Aadhaar number is 1234455, and my PAN Number is adf1234."

"Thank you, Sir. Please wait. I am registering your Aadhaar and PAN, you will get a registration OTP code. Please share that."

Raju received an SMS- your verification code is 1234

"Yes, it is 1234."

"Thank you, Sir. You have been successfully registered for the vaccine, and you will get a confirmation soon. Please share the code when our health officials visit to vaccinate you."

The call got disconnected. After some time, Raju got an SMS

'Dear Customer, your request for a personal loan of Rs 50,000 has been successfully accepted.'

The fraudster tricked Raju into sharing his PAN number and OTP for taking a loan of Rs. 50,000/- on behalf of Raju. Taking a loan based on Raju's PAN number makes Raju liable to pay back the loan to XYZ Company.

Don'ts:

- × Don't share your Aadhaar, PAN and OTP with strangers.

PAN card-based OTP is used for various financial services including cash withdrawals from bank accounts. Therefore, it is extremely important to protect your confidential details such as Aadhaar and PAN numbers 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.

"Hello, I want to book a Covid-19 test."



"Welcome to ABC Diagnostics.  
Please provide your address for sample collection."



"My address is 25, ABC Lane, Mumbai, Maharashtra. What will be the cost for the test?"



"It will cost Rs. 1,000/- plus home collection charge of Rs. 100/-. Also, you must pay Rs. 550/- in advance for pre-booking. I will share the payment link for pre-booking with you."



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

Raju had bought a motorcycle using a vehicle loan availed from XYZ Bank. However, Raju lost his job and was struggling to repay the loan EMIs. One day a fraudster disguised as a recovery agent of XYZ Bank approached Raju at his residence.

Fraudster: "I am a recovery agent from XYZ Bank. It is seen that you have defaulted repayment of loan dues. I am here to officially seize your vehicle."



Raju: "Oh, no! Please don't seize my vehicle. I have missed last few EMIs as I had lost my job. I have got a new job offer at hand and I promise to repay from next month."

"No, No! This is bank's procedure. You have around Rs. 20,000/- as dues. You will have to pay at least Rs. 5,000/- now or I will have to take the vehicle."

**Do's:**

- ✓ Always ensure identification of Recovery Agents before making any payment / commitment. Check whether the 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 incident to the nearest Police Station and your home branch.



<p>Fraudster collects money:</p> <p>"Okay. I will pay Rs. 5,000/- now and remaining in the next few months."</p>  <p>"Ok, sir. I am doing this as a special favour. You can collect the receipt and pending dues position directly from the bank branch"</p>	<p>After few days another recovery agent approaches Raju at his residence:</p>  <p>"Good evening, Sir. I am Ravi, Recovery Agent from XYZ Bank. Please see this recovery notice issued by bank stating that you have missed your last three EMIs and bank may go forward with seizure of vehicle. You may either pay directly at the bank or pay it to me against receipt."</p>
<p>"How come? I have already paid Rs. 5,000/- a few days before to your agent."</p> 	<p>"That is not possible sir. I am the authorised agent for XYZ bank in this area. Please see my ID Card and the authorization letter from the bank for recovering dues. Did you see his ID? Do you have any proof of making payment?"</p>  <p>"Oh, No! I trusted him blindly"</p>
<p>Don't's</p> <ul style="list-style-type: none"><li>✗ Never make any cash payments to bank / recovery agents without proper acknowledgement of receipt.</li></ul>	



## 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 for around Rs. 12,000/- are lying unused with us."

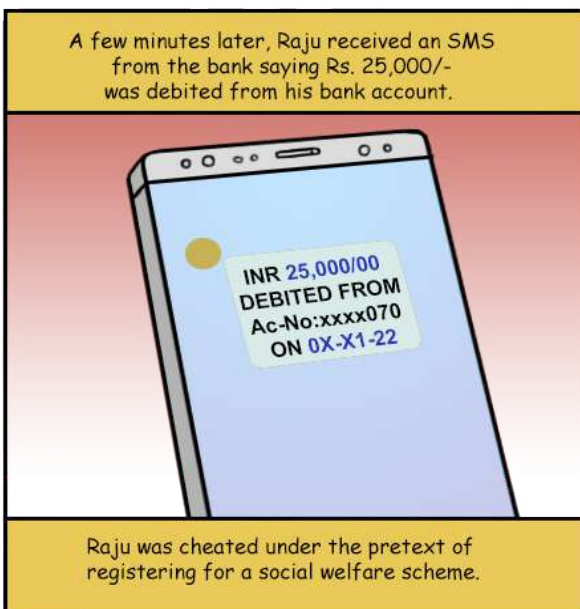
"What should I do to update the account?"

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



### 23. MULTI-LEVEL MARKETING (MLM) SCAMS

Raju's friend Krishna visited him to explain about a scheme with good earning potential.

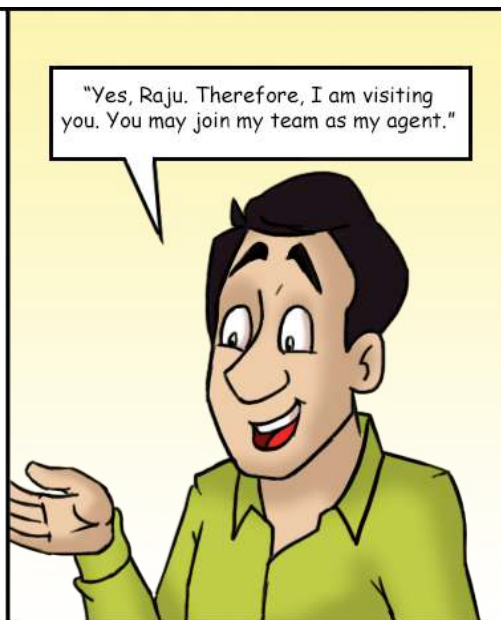
"Hi Raju! I came across a fantastic opportunity to make money with minimal time and investment."

"Is it? Sounds exciting! Tell me more about it. I want to know everything."

"You must buy XYZ company products for Rs 20,000/- and you will get a mobile phone of Rs 10,000/- for free. After you enrol three more people, you will get a commission of Rs. 3,000/- per person as you bring more and more people under the scheme."

**Do's:**

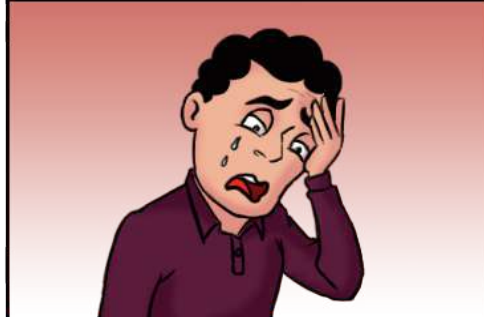
- ✓ Stay away from people trying to get you into these kinds of schemes.
- ✓ Verify the authenticity of the Multi Level Marketing scheme. Some of the network marketing schemes, like Ponzi scheme, Pyramid scheme etc., are illegal in India under the Direct Selling Guidelines, 2016 and the Prize Chits and 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>.



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 non-existent. He could not accomplish the targets set by the company of recruiting 3 more agents, and he lost Rs. 20,000/- as the products bought by him from the company 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.

## 24. WORK FROM HOME SCAM

A fraudster advertises jobs over the internet and social media with attractive pay for working from home. (Earn Rs. 1,000/- per day working from home).



Raju is very excited after coming across the advertisement and clicks on the link to register for work from home. Raju receives a call from a stranger.



"Sir, thank you for registering with our agency. We have gone through your CV, and you are selected for the work from home job. You need to provide your Aadhaar and PAN card details. You will also have to fill up some forms and sign some documents as per our company policy."

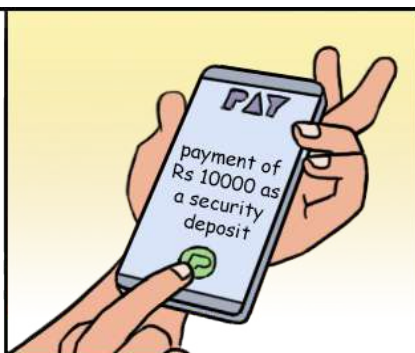


"Thank you. I will fill all the forms and send you my address proof and PAN card details."



### Do's:

- ✓ Beware of short URLs, information requested on Google forms from unknown sources.
- ✓ Look for poor spelling, grammar in emails, SMS, and portals, as fraudsters might be imitating genuine companies.
- ✓ 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. 10,000/- as a security deposit to the fraudster. The job progresses smoothly for a week. Raju kept receiving regular payments. He got Rs. 7,000/- 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.



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

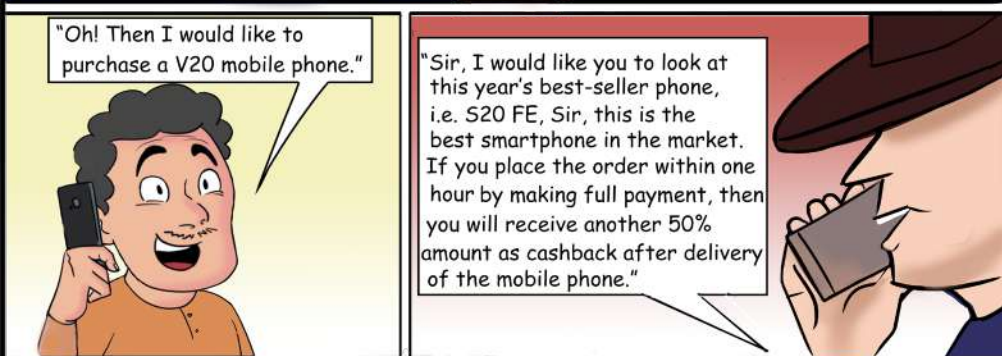


He got calls threatening legal action and then, terrified with all this, Raju paid Rs 1 lakh to the fraudster.

- 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 as 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>.



<p>"Okay. What is the price of the phone??"</p> 	<p>"Sir, the current market price of the phone having the same features is more than one lakh, but we are selling the same for just Rs. 50,000/- . You will receive a cashback of Rs. 25,000/-"</p> 	
<p>"Okay. I will think about the same and let you know."</p> 	<p>"Sir, this offer is valid for the next 50 minutes, and only a few phones are left in stock. You must place an order immediately and make payment to avail the offer."</p> 	
<p>Raju reasoned he can't afford a phone costing Rs. 50,000/-, but he again thought that he will receive 50% as cashback after delivery of the mobile phone; so this is an excellent deal for him.</p>		
<p>"Okay, I will immediately make the payment."</p> 	<p>"That's a great decision, Sir. I am sending you a link for payment. Please make your payment at the earliest."</p> 	<p>Raju made the payment and waited for the delivery of the product, But he never received any mobile !</p> 
<p><b>Don'ts:</b></p> <ul style="list-style-type: none"><li>× Never do online shopping from unknown websites.</li><li>× 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.</li><li>× Never pay in advance to unknown sites, as chances of getting a product are negligible after payment has been done.</li></ul>		

## 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. 12,000/-, 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>.



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



Raju was happy. His day was well spent. After some time, he started receiving SMS alerts from his bank. 'Rs. 14,000/- and Rs. 10,000/- were debited from your account.' Raju was confused.

The last transaction he made was for Rs. 12,000/- at the mall, and these transactions were different. He told his son about the messages.



"I made the last transaction at the shopping mall; I paid the bill online. My network was not working, so I connected to a free Wi-Fi and made the payment."

"You used free Wi-Fi for a financial transaction? That is not safe, Dad. Hackers use this Wi-Fi to get access to users data and use it for illegal"



"When you used the Wi-Fi network for the financial transaction, some hacker got access to your personal data and used it for unauthorized transactions from your bank account. This is the reason you are getting these messages."

"Oh God! I made a big mistake. What can we do now?"

"We must immediately visit your bank and ask them to block your account."

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

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  
the product at your address."



Do's:

- ✓ In the case of branded products, verify the advertisements using 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 already shared them. I have also shared account details for transferring the amount. You must pay Rs. 3,000/- to confirm the order. Once the 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 the watches 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 if buying from unverified sources.



## 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 for up to Rs 5 lakhs at an interest rate 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 the 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. 5,000/- immediately to avail 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 of 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

"Hello, Mr Raju. I am calling from XYZ Bank. Congratulations on your new credit card, Sir!"

"Yes, thanks. I received it."

Raju recently received a XYZ bank credit card

"As per bank's policy, I am contacting you to activate your new credit card through call. You need to confirm the details of your card, following which you will receive an activation code. Upon entering the code, your card will be activated."

Raju believed the fraudster as he already had his credit card details

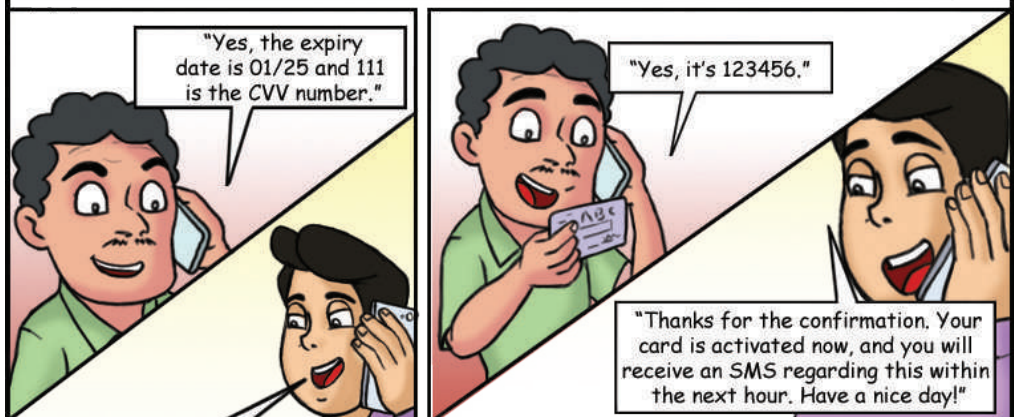
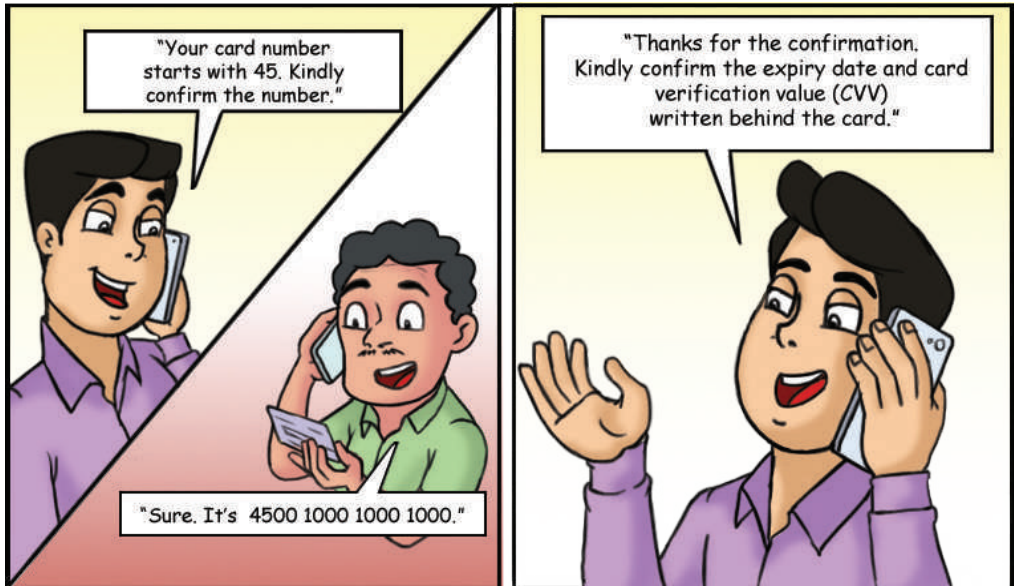
"Okay. Please activate my card."

"Your name is Raju Deshpande. Your address is Lower Parel, Mumbai?"

"That's correct."

**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 incident.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



"Thanks for the confirmation, Sir. You must have received an SMS for the final activation. Kindly confirm the code received on your phone."

Raju received an SMS from his bank, about debit of Rs 1.2 lakhs on his credit card. Here, Raju was defrauded under the pretext of credit card activation.

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



### 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."

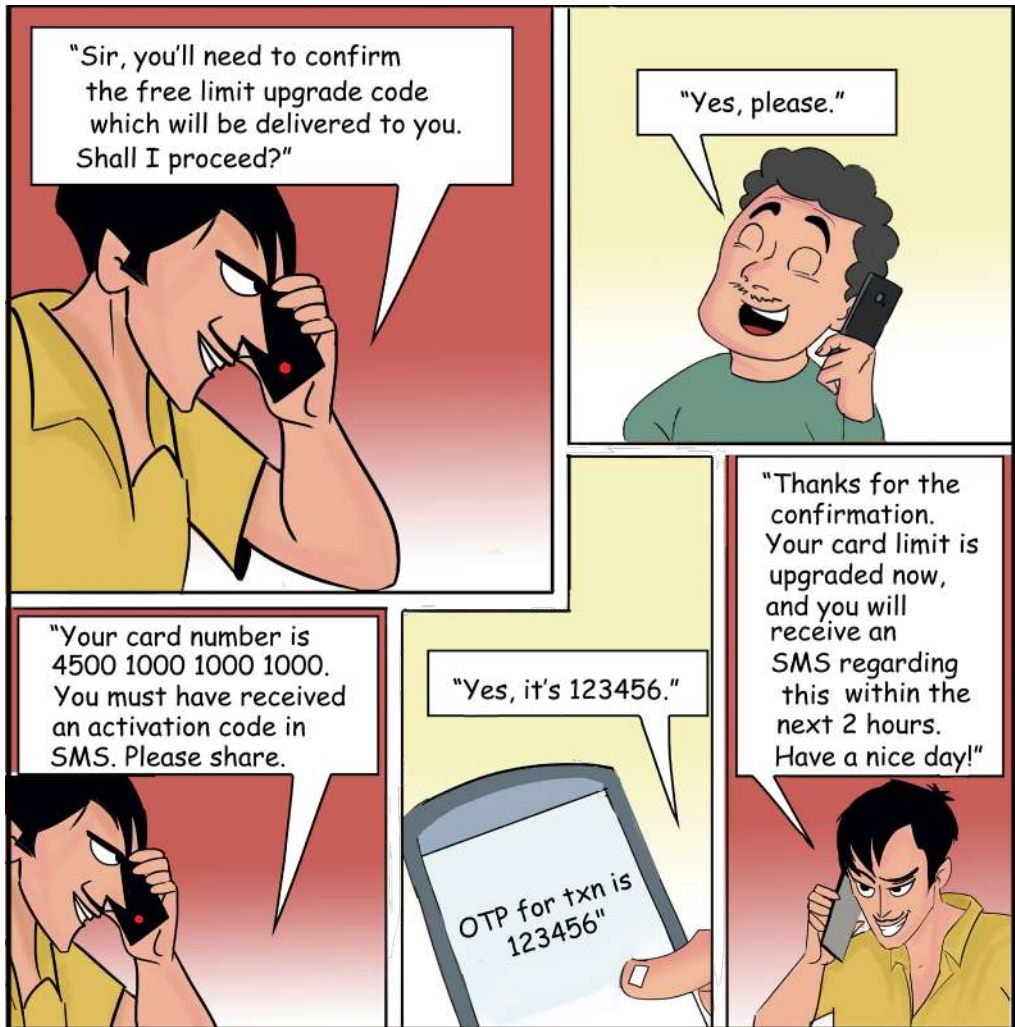


"Oh, that's great!"



**Do's:**

- ✓ After realising that a fraud has occurred, 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 a debit of Rs. 70,000/- 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

One day, Raju went to his bank branch to get his Aadhaar card linked with his bank account.

"I want to link my Aadhaar card with my bank account."

Raju submits the required documents.

"Please submit the Aadhaar linking form and photocopy of your Aadhaar card. Also, show me your original Aadhaar card."

"Tell me the OTP you received on your registered mobile number."

"I did not get any OTP."

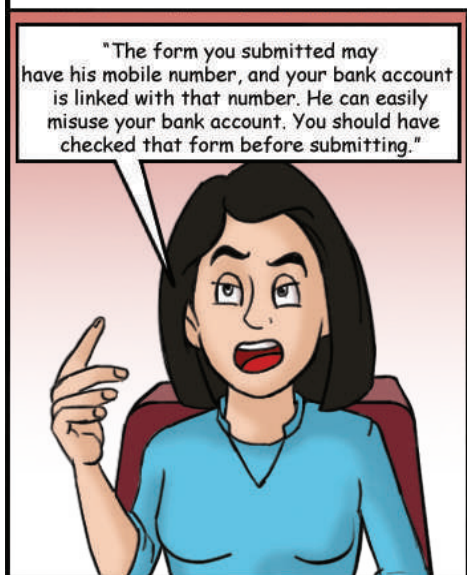
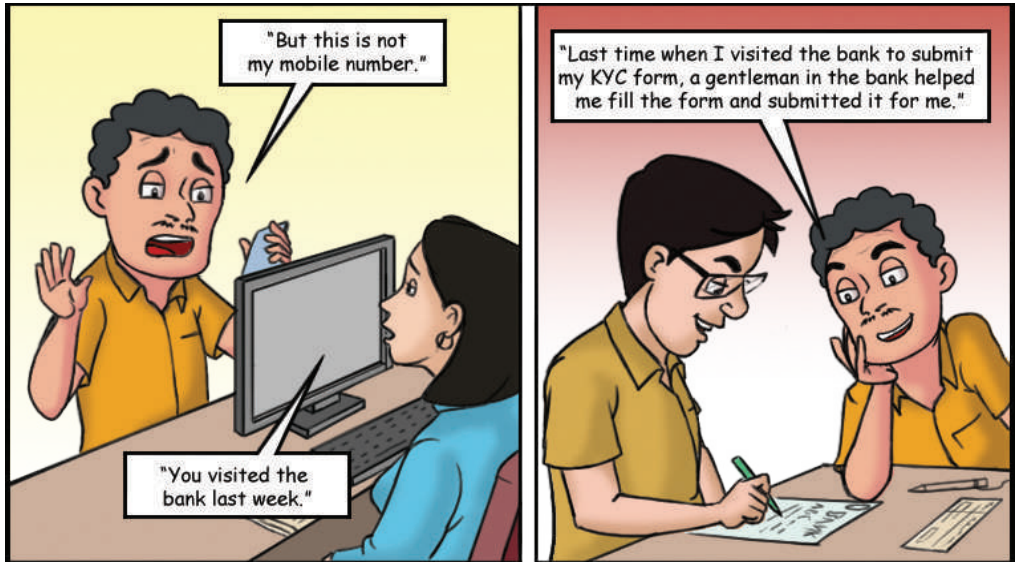
"The OTP was sent to your registered mobile number."

"But I did not receive any OTP. Can you please check the mobile number linked to my bank account?"

"Let me check. The mobile number linked to your account is 98\*\*\*25621."

**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>.



Don'ts-

- ✗ Don't share your confidential details like Aadhaar and bank account details with strangers.
- ✗ Don't take the help of strangers to carryout transactions / submit forms at bank. Avail the help of bank officials only and verify the details before submitting.



## 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 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 UPI app and there will be a pop-up message regarding the cashback."



Dos-

- ✓ As soon as identifying a fraud, 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 for Rs. 20,000/- to abc.com"

"That is correct, Sir. We must take your approval to credit cashback in to 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 the 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.



### 33. DISCOUNT FRAUD

Raju wanted to book a hall for his daughter's birthday party. So he searched on the internet for the available options and entered details for enquiry. After a few moments, Raju got a call.

"Hello, I am speaking from XYZ Hotel. You inquired about bookings on our website. How can I help you?"

"I wanted to ask about the banquet hall at your hotel. Is it available on rent?"

"Yes, rental options are available for the banquet hall."

"What are the charges? I want to book it for my daughter's birthday."

"We charge on an hourly basis. It is Rs. 2,500/- per hour."

"Is it available on xx-xx-xx date, from 8 p.m. to 10 p.m.?"

"Yes Sir, It is available. As a pre-booking fee, you will have to send me Rs. 1,000/- to generate a token number."

"I will come to your office to make the payment."

**Dos-**

- ✓ Always verify the authenticity of the person / institution advertising 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>.



After some time, Raju received an SMS alert on his phone. 'Rs. 50,000/- was debited from your account.' Raju immediately called the person, but he did not answer. Raju realized that the person was a fraudster, and he should not have shared any card details with him.

Don'ts-  
X 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.

**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 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 regarding your charity providing smartphones 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 our 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.



### 35. OVERDRAFT AGAINST FD

Raju is a senior citizen, who had recently retired from his job and received a large sum of superannuation money, which he wanted to invest. One day, Raju received a call from someone, pretending to be the employee / agent of a reputed bank, advertising a new scheme with a high interest rate.



"Hello! Are you sure I will get a 9% interest rate? Because no bank is giving more than 7.1% interest."

"Yes, sir. This is a special scheme for a limited period only."



Raju: "Okay, I will visit the bank and open a Fixed deposit."

Raju: "No, I can't hand over my money to an unknown person."

"Sir, our bank will send a representative to your home since you are a senior citizen."



Do's:

- ✓ Check all documents before signing them.
- ✓ Prefer visiting the bank branch or perform transactions over internet banking.
- ✓ 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 persons.

## 36. FRAUDS USING MALICIOUS APPLICATION

One day, Raju received a message seeking his willingness to do freelance work. As Raju was unemployed, he immediately dialed 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 the 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 an SMS alert stating that 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.

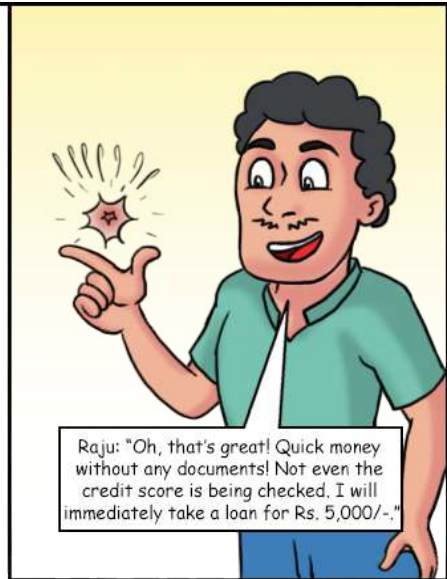


Don'ts:

- ✗ 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 and Ramu were best friends. One day, Raju met Ramu and told him about his financial problems.



Raju downloads a mobile app without verifying whether the entity providing loan is a registered one. He gets Rs. 5,000/- 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 at [https://www.rbi.org.in/Scripts/BS\\_NBFCList.aspx](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/>.

Within 7 days, Raju started receiving calls for repayment of Rs. 7,500/-.  
Raju still had not arranged money to repay the old loan and gets shocked by the demand for Rs. 7,500/- as repayment for a loan of Rs. 5,000/-.  
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.

"Welcome, Sir.  
Please have a seat."

"Thank You."

"How can I  
help you, sir?"

"Could I see your  
menu card?"

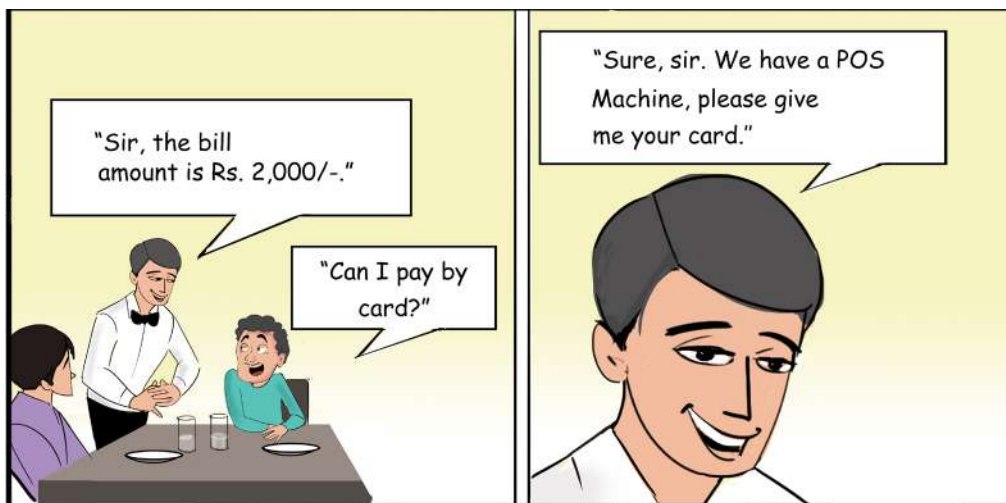
"Sure, sir.  
This is our menu card."

Raju ordered food and enjoyed  
the meal with his friends.

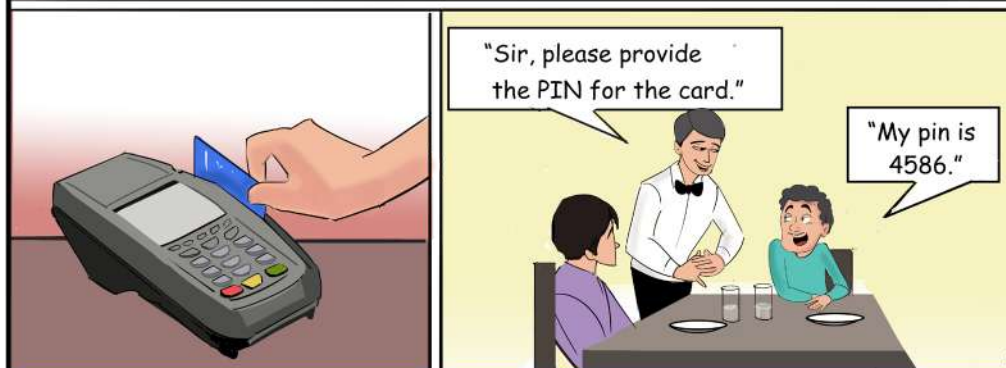
"Please get the bill."

### Do's:

- ✓ Always hide your pin number while carrying out transactions through debit / credit cards.
- ✓ 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.

"Hello, Raju. Are you free to talk?"

"Yes, Keshav; tell me."

"There is an exciting offer on xyz e-commerce website. It requires a creditcard issued by abc bank. You are using this card. Can you send me the details of your credit card over phone? I will pay you later."

"Okay I will send the details of my card."

"I received your card details. Thank you so much."


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."



"Oh! Keshav, you should have told me about this incident. I would have blocked the card. I should not have shared my card details over the phone."

Not clear how transactions happened without OTP, Raju realised that he himself had never done any payment on 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.



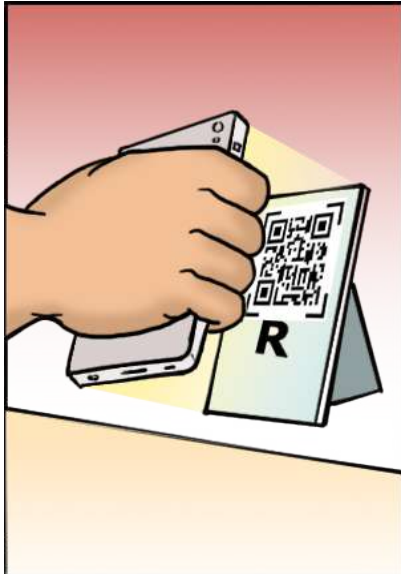
## 40. PAYMENT SPOOFING APPLICATIONS.

Raju is a friendly retail shop owner. He was sitting at his shop when a customer came and purchased something.



### 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."



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 any financial transaction without actual receipt of fund.





Consumer Education and Protection  
Department (CEPD), RBI

<https://cms.rbi.org.in/>