


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!

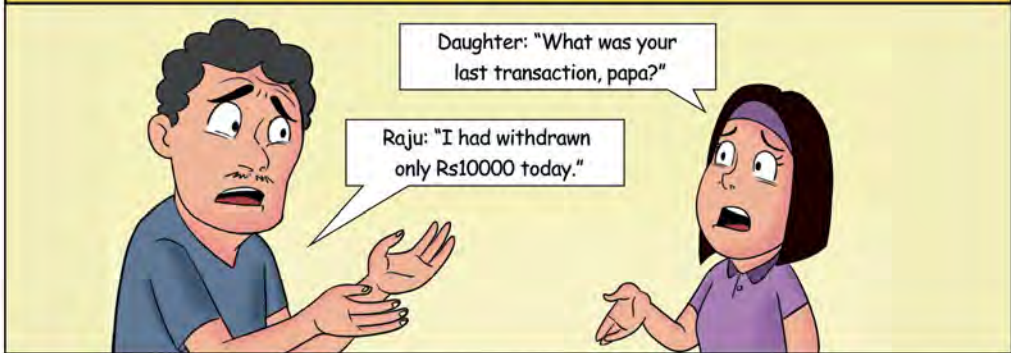
Raju withdraws the money, and he gets an SMS alert for his transaction.

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.)



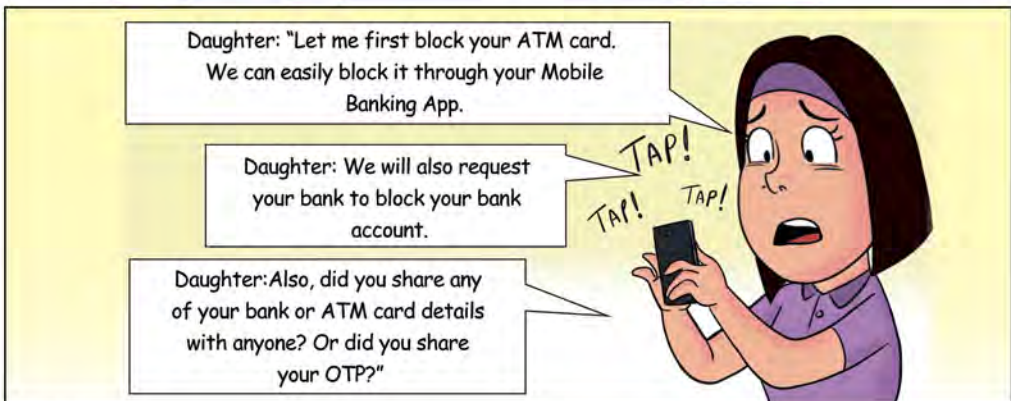
Raju: "This SMS is about a transaction with my ATM card. But I have used it only once today."

Raju tells his daughter about the SMS alerts.



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

Raju: "I had withdrawn only Rs10000 today."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.

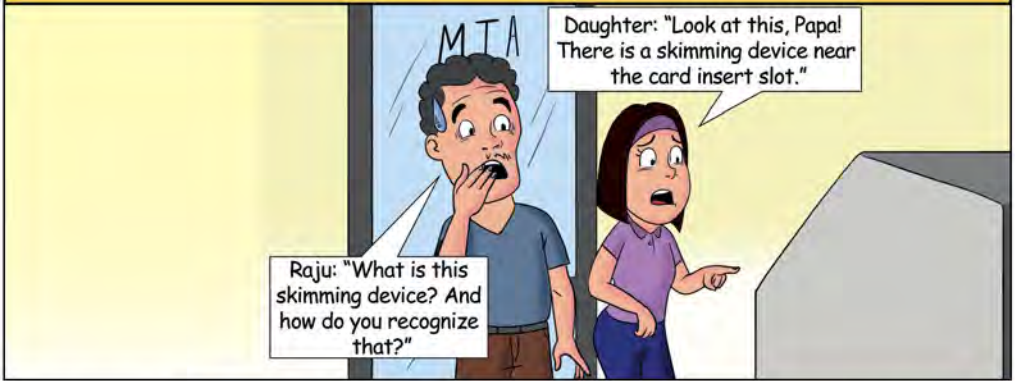
Daughter: Also, did you share any of your bank or ATM card details with anyone? Or did you share your OTP?"

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 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.



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.