

# Customer Awareness Brochure



सहकारातून समृद्धी

---

**MSC BANK**  
SCHEDULED BANK



## Table of Contents

	Subject	Page No.
	<a href="#">Preface</a>	1
	<a href="#">Part A - Modus Operandi and Precautions to be taken against Fraudulent Transactions - Banks</a>	2
1	<a href="#">Phishing links</a>	3
2	<a href="#">Vishing calls</a>	4
3	<a href="#">Frauds using online sales platforms</a>	5
4	<a href="#">Frauds due to the use of unknown / unverified mobile apps</a>	6
5	<a href="#">ATM card skimming</a>	7
6	<a href="#">Frauds using screen sharing app / Remote access</a>	8
7	<a href="#">SIM swap / SIM cloning</a>	9
8	<a href="#">Frauds by compromising credentials through search engines</a>	10
9	<a href="#">Scam through QR code scan</a>	11
10	<a href="#">Impersonation on social media</a>	12
11	<a href="#">Juice jacking</a>	13
12	<a href="#">Lottery frauds</a>	14
13	<a href="#">Online job frauds</a>	15
14	<a href="#">Money mules</a>	16



## Preface

There has been a surge in usage of digital modes of payment in the recent years. This gained further momentum during the Covid-19 induced lockdowns. While enhancing customer convenience, it also furthered the national objective of financial inclusion. However, as the speed and ease of doing financial transactions has improved, the number of frauds reported in retail financial transactions have also gone up. Fraudsters have been using innovative methods to defraud the common and gullible people of their hard-earned money, especially the new entrants in the use of digital platforms who are not entirely familiar with the techno-financial eco-system.

This booklet has been compiled from various incidents of frauds reported as also from complaints received at the offices of RBI Ombudsmen to provide maximum practical information of value, especially to those who are inexperienced, or not so experienced, in digital and electronic modes of financial transactions. The booklet is intended to create awareness among the members of public about the modus operandi adopted by fraudsters to defraud and mislead them, while also informing them about the precautions to be taken while carrying out financial transactions. It emphasizes the need for keeping one's personal information, particularly the financial information, confidential at all times, be-ware of unknown calls / emails / messages, practicing due diligence while performing financial transactions and changing the secure credentials / passwords from time to time. Hence the title **BE(A)WARE** – Be Aware and Beware!

This booklet is part of the public awareness initiative by the Consumer Education and Protection Department, Reserve Bank of India and has been conceptualized by the office of Ombudsman, Mumbai-II.



## Modus Operandi and Precautions to be taken against Fraudulent Transactions - Banks



## 1. Phishing links

### Modus Operandi

- Fraudsters create a third-party phishing website which looks like an existing genuine website, such as - a bank's website or an e-commerce website or a search engine, etc.
- Links to these websites are circulated by fraudsters through Short Message Service (SMS) / social media / email / Instant Messenger, etc.
- Many customers click on the link without checking the detailed Uniform Resource Locator (URL) and enter secure credentials such as Personal Identification Number (PIN), One Time Password (OTP), Password, etc., which are captured and used by the fraudsters.



### Precautions

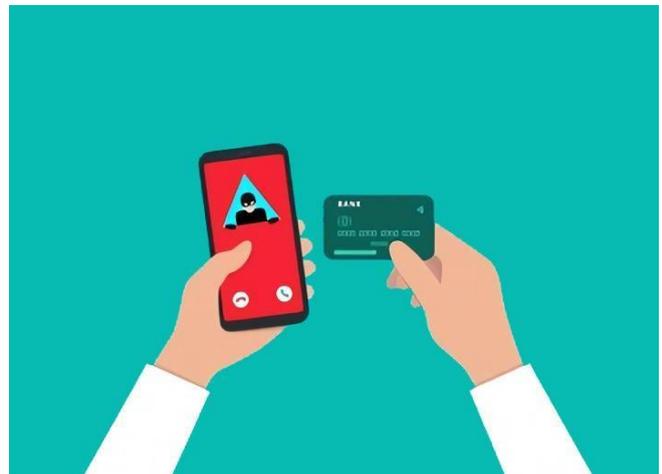
- Do not click on unknown / unverified links and immediately delete such SMS / email sent by unknown sender to avoid accessing them by mistake in future.
- Unsubscribe the mails providing links to a bank / e-commerce / search engine website and block the sender's e-mail ID, before deleting such emails.
- Always go to the official website of your bank / service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials.
- Check URLs and domain names received in emails for spelling errors. In case of suspicion, inform



## 2. Vishing calls

### Modus Operandi

- Imposters call or approach the customers through telephone call / social media posing as bankers / company executives / insurance agents / government officials, etc. To gain confidence, imposters share a few customer details such as the customer's name or date of birth.
- In some cases, imposters pressurize / trick customers into sharing confidential details such as passwords / OTP / PIN / Card Verification Value (CVV) etc., by citing an urgency / emergency such as - need to block an unauthorised transaction, payment required to stop some penalty, an attractive discount, etc. These credentials are then used to defraud the customers.



### Precautions

- Bank officials / financial institutions / RBI / any genuine entity never ask customers to share confidential information such as username / password / card details / CVV / OTP.
- Never share these confidential details with anyone, even your own family members, and friends.

### 3. Frauds using online sales platforms

#### Modus Operandi

- Fraudsters pretend to be buyers on online sales platforms and show an interest in seller's product/s. Many fraudsters pretend to be defence personnel posted in remote locations to gain confidence.
- Instead of paying money to the seller, they use the "request money" option through the Unified Payments Interface (UPI) app and insist that the seller approve the request by entering UPI PIN. Once the seller enters the PIN, money is transferred to the fraudster's account.



#### Precautions

- Always be careful when you are buying or selling products using online sales platforms.
- Always remember that there is **no need to enter PIN / password** anywhere to **receive** money.
- If UPI or any other app requires you to enter PIN to complete a transaction, it means you will be sending money instead of receiving it.

#### 4. Frauds due to the use of unknown / unverified mobile apps

##### Modus Operandi

- Fraudsters circulate through SMS / email / social media / Instant Messenger, etc., certain app links, masked to appear similar to the existing apps of authorised entities.
- Fraudsters trick the customer to click on such links which results in downloading of unknown / unverified apps on the customer's mobile / laptop / desktop, etc.,
- Once the malicious application is downloaded, the fraudster gains complete access to the customer's device. These include confidential details stored on the device and messages / OTPs received before / after installation of such apps.



##### Precautions

- Never download an application from any unverified / unknown sources or on being asked/ guided by an unknown person.
- As a prudent practice before downloading, check on the publishers / owners of the app being downloaded as well as its user ratings etc.
- While downloading an application, check the permission/s and the access to your data it seeks, such as contacts, photographs, etc. Only give those permissions which are absolutely required to use the desired application.



## 5. ATM card skimming

### Modus Operandi

- Fraudsters install skimming devices in ATM machines and steal data from the customer's card.
- Fraudsters may also install a dummy keypad or a small / pinhole camera, well-hidden from plain sight to capture ATM PIN.
- Sometimes, fraudsters pretending to be other customer standing near-by gain access to the PIN when the customer enters it in an ATM machine.
- This data is then used to create a duplicate card and withdraw money from the customer's account.



### Precautions

- Always check that there is no extra device attached, near the card insertion slot or keypad of the ATM machine, before making a transaction.
- Cover the keypad with your other hand while entering the PIN.
- NEVER write the PIN on your ATM card.
- Do NOT enter the PIN in the presence of any other / unknown person standing close to you.
- Do NOT give your ATM card to anyone for withdrawal of cash.
- Do NOT follow the instructions given by any unknown person or take assistance / guidance from strangers / unknown persons at the ATMs.
- If cash is not dispensed at the ATM, press the 'Cancel' button and wait for the home screen to appear before leaving the ATM.

## 6. Frauds using screen sharing app / Remote access

### Modus Operandi

- Fraudsters trick the customer to download a screen sharing app.
- Using such app, the fraudsters can watch / control the customer's mobile / laptop and gain access to the financial credentials of the customer.
- Fraudsters use this information to carry out unauthorised transfer of funds or make payments using the customer's Internet banking / payment apps.



### Precautions

- If your device faces any technical glitch and you need to download any screen sharing app, deactivate / log out of all payment related apps from your device.
- Download such apps only when you are advised through the official Toll-free number of the company as appearing in its **official website**. Do not download such apps in case an executive of the company contacts you through his / her personal contact number.
- As soon as the work is completed, ensure that the screen sharing app is removed from your device.

## 7. SIM swap / SIM cloning

### Modus Operandi

- Fraudsters gain access to the customer's Subscriber Identity Module (SIM) card or may obtain a duplicate SIM card (including electronic-SIM) for the registered mobile number connected to the customer's bank account.
- Fraudsters use the OTP received on such duplicate SIM to carry out unauthorised transactions.
- Fraudsters generally collect the personal / identity details from the customer by posing as a telephone / mobile network staff and request the customer details in the name of offers such as - to provide free upgrade of SIM card from 3G to 4G or to provide additional benefits on the SIM card.



### Precautions

- Never share identity credentials pertaining to your SIM card.
- Be watchful regarding mobile network access in your phone. If there is no mobile network in your phone for a considerable amount of time in a regular environment, immediately contact the mobile operator to ensure that no duplicate SIM is being / has been issued for your mobile number.

## 8. Frauds by compromising credentials on results through search engines

### Modus Operandi

- Customers use search engines to obtain contact details / customer care numbers of their bank, insurance company, Aadhaar updation centre, etc. These contact details on search engines often do NOT belong to the respective entity but are made to appear as such by fraudsters.
- Customers may end up contacting unknown / unverified contact numbers of the fraudsters displayed as bank / company's contact numbers on search engine.
- Once the customers call on these contact numbers, the imposters ask the customers to share their card credentials / details for verification.
- Assuming the fraudster to be a genuine representative of the RE, customers share their secure details and thus fall prey to frauds.



### Precautions

- Always obtain the customer care contact details from the official websites of banks / companies.
- Do not call the numbers directly displayed on the search engine results page as these are often camouflaged by fraudsters.
- Please also note that customer care numbers are never in the form of mobile numbers.

## 9. Scam through QR code scan

### Modus Operandi

- Fraudsters often contact customers under various pretexts and trick them into scanning Quick Response (QR) codes using the apps on the customers' phone.
- By scanning such QR codes, customers may unknowingly authorise the fraudsters to withdraw money from their account.



### Precautions

- Be cautious while scanning QR code/s using any payment app. QR codes have account details embedded in them to transfer money to a particular account.
- Never scan any QR code to receive money. Transactions involving receipt of money do not require scanning barcodes / QR codes or entering mobile banking PIN (m-PIN), passwords, etc.

## 10. Impersonation on social media

### Modus Operandi

- Fraudsters create fake accounts using details of the users of social media platforms such as Facebook, Instagram, Twitter, etc.
- Fraudsters then send a request to the users' friends asking for money for urgent medical purposes, payments, etc.
- Fraudsters, using fake details, also contact users and gain users' trust over a period of time. When the users' share their personal or private information, the fraudsters use such information to blackmail or extort money from the users.



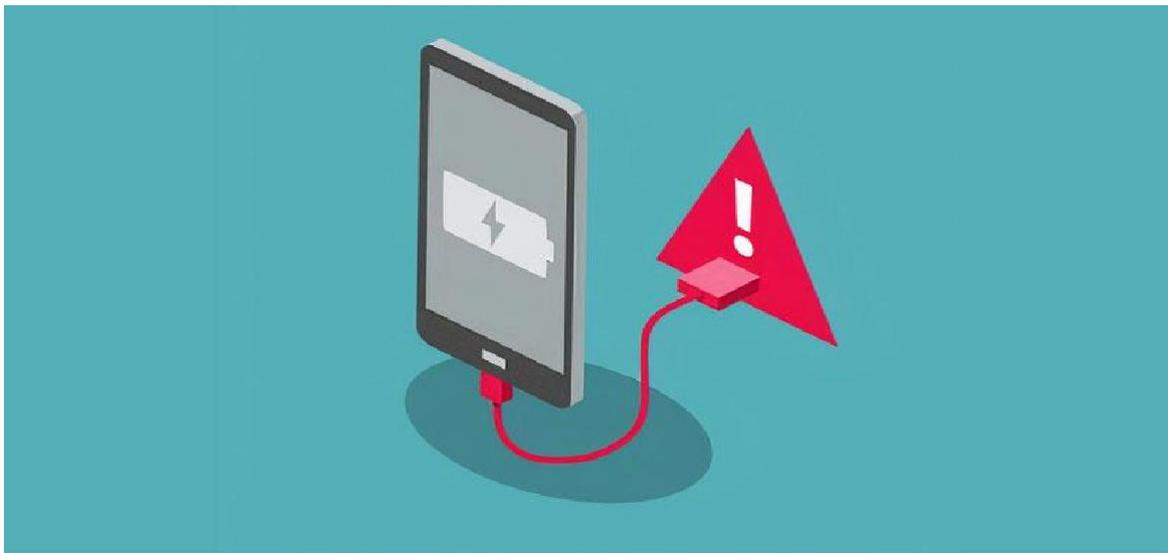
### Precautions

- Always verify the genuineness of a fund request from a friend / relative by confirming through a phone call / physical meeting to be sure that the profile is not impersonated.
- Do not make payments to unknown persons online.
- Do not share personal and confidential information on social media platforms.

## 11. Juice jacking

### Modus Operandi

- The charging port of a mobile, can also be used to transfer files / data.
- Fraudsters use public charging ports to transfer malware to customer phones connected there and take control / access / steal data sensitive data such as emails, SMS, saved passwords, etc. from the customers' mobile phones (Juice Jacking).



### Precaution

- Avoid using public / unknown charging ports / cables.



## 12. Lottery fraud

### Modus Operandi

- Fraudsters send emails or make phone calls that a customer has won a huge lottery. However, in order to receive the money, the fraudsters ask the customers to confirm their identity by entering their bank account / credit card details on a website from which data is captured by the fraudsters.
- Fraudsters also ask the customers to pay taxes/ forex charges / upfront or pay the shipping charges, processing / handling fee, etc., to receive the lottery / product.
- Fraudsters in some cases, may also pose as a representative of RBI or a foreign bank / company / international financial institution and ask the customer to transfer a relatively small amount in order to receive a larger amount in foreign currency from that institution.
- Since the requested money is generally a very small percentage of the promised lottery / prize, the customer may fall into the trap of the fraudster and make the payment.



### Precautions

- Beware of such unbelievable lottery or offers - nobody gives free money, especially such huge amounts of money.
- Do not make payments or share secure credentials in response to any lottery calls / emails.
- RBI never opens accounts of members of public or takes deposits from them. Such messages are fraudulent.
- RBI never asks for personal / bank details of members of public. Beware of fake RBI logos and messages.
- Never respond to messages offering / promising prize money, government aid and Know Your Customer (KYC) updation to receive prize money from banks, institutions etc.

### 13. Online job fraud

#### Modus Operandi

- Fraudsters create fake job search websites and when the job seekers share secure credentials of their bank account / credit card / debit card on these websites during registration, their accounts are compromised.
- Fraudsters also pose as officials of reputed company(s) and offer employment after conducting fake interviews. The job seeker is then induced to transfer funds for registration, mandatory training program, laptop, etc.



#### Precautions

- For any job offer, including from overseas entities, first confirm the identity and contact details of the employing company / its representative.
- Always remember that a genuine company offering a job will never ask for money for offering the job.
- Do not make payments on unknown job search websites.

## 14. Money mules

### Modus Operandi

- Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen / illegal money via their bank account/s.



- Fraudsters contact customers via emails, social media, etc., and convince them to receive money into their bank accounts (money mule), in exchange for attractive commissions.
- The money mule is then directed to transfer the money to another money mule's account, starting a chain that ultimately results in the money getting transferred to the fraudster's account.
- Alternatively, the fraudster may direct the money mule to withdraw cash and hand it over to someone.
- When such frauds are reported, the money mule becomes the target of police investigation for money laundering.

### Precautions

- Do not allow others to use your account to receive or transfer money for a fee / payment.
- Do not respond to emails asking for your bank account details.
- Do not get carried away by attractive offers / commissions and give consent to receive unauthorised money and to transfer them to others or withdraw cash and give it out for a handsome fee.
- If the source of funds is not genuine, or the rationale for underlying transaction is not proved to authorities, the receiver of money is likely to land in serious trouble with police and other law enforcement agencies.

**THE END**