



**Saraswat
Bank**

SATARK BANKING

— BE VIGILANT, BE SAFE —

A GUIDE FOR
**SATARK
BANKING**
AN INITIATIVE FOR CUSTOMER EDUCATION



**Saraswat
Bank**

Saraswat Co-operative Bank Ltd.
(Scheduled Bank)



**Saraswat
Bank**

SATARK BANKING

— BE VIGILANT, BE SAFE —

TABLE OF CONTENTS

Acknowledgements	01
Preface	01
General Guidelines	02
Phishing	03
Vishing	04
SMSHING	05
SIM Swap Attack	06
QR Code Frauds	07
ATM Card Skimming	08
Impersonating Through Social Media	09
Frauds Using Online Selling Platforms	10
Fake Loan Websites/App	11
Money Mule	12
Fraud by Remote Access	13
Fraudulent Loans with Forged Documents	14
Juice Jacking	15



**Saraswat
Bank**

SATARK BANKING

— BE VIGILANT, BE SAFE —

ACKNOWLEDGEMENTS

The contents of the document are taken from, 'A Booklet on Modus Operandi of Financial Fraudsters' released by the Office of the RBI Ombudsman (Mumbai-II) Maharashtra, Goa and some of our in-house research on this subject matter.

PREFACE

With so many people using the Internet and mobile apps for banking, it helps to know that security is important, especially with regards to financial transactions where it is vital to guard against any exploitation.

Since our customer's information and financial security is our top priority, we are committed to secure the same and also encourage you to be Satark and have a secure and safe banking experience.

With this endeavour of having a dedicated booklet, we have a focused approach to make our customers as well as the larger audience aware about increasingly sophisticated and malicious techniques being attempted by attackers / fraudsters and top security preventive measures.

We believe your support in being vigilant will also serve as mutual harmony.



GENERAL GUIDELINES



Password Security

- » Create at least an 8 character long password including numbers, special characters & a capital letter
- » Have different passwords for business & personal use
- » Change your password at regular intervals
- » Never share your Password



Online Banking

- » Login to your e-banking account only via official website of the bank
- » Use a mixture of letters & numbers & symbols as your password
- » Don't use public Wi-Fi & computers while banking online
- » Check your bank statement Regularly



Phone Banking

- » Never share your personal details in a public place, or to an unknown/unverified source
- » Call only on **1800229999**, if you are trying to call Saraswat Bank via toll free number



E-Mail Security

- » Never respond to unverified or spam emails
- » If you feel you have received any email which claims to be from Saraswat Bank but looks suspicious, kindly report the same to corporatecenter@saraswatbank.com



Mobile Banking

- » Always set a password on your mobile device
- » Turn off your Wi-Fi, Bluetooth, GPS, when not in use
- » Never visit unverified websites & never download apps from unverified sources



ATM Banking

- » Change the PIN as you receive a new card from the bank
- » Don't write or share your PIN/CVV/OTP
- » Change your PIN at regular Intervals



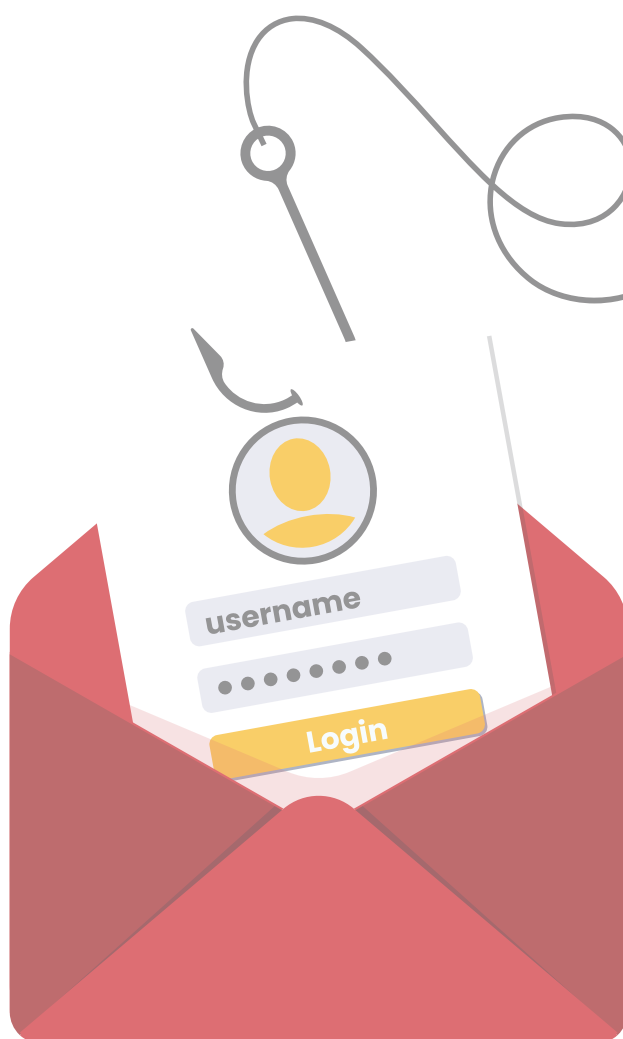
PHISHING

How the Scam Happens

- » Genuine websites of banks, e-commerce, even search engines are cloned into fake replicas.
- » Fraudulent links are circulated via SMSs, Social Media, Emails or other Messengers.
- » Fake URLs are masked behind authentic-looking names while Phishing Websites appear exact replica of a genuine one.
- » If an individual clicks on such fake link and enters credentials, this information is then available to the phisher / scamster.

Precautions

- » Verify websites especially when it asks for financial credentials. A secure website should start with "https://" where 's' stands for secure.
- » Never click unknown links received through SMS, emails, and other instant messengers.
- » Delete suspicious SMS/email immediately to avoid even accidental future use.





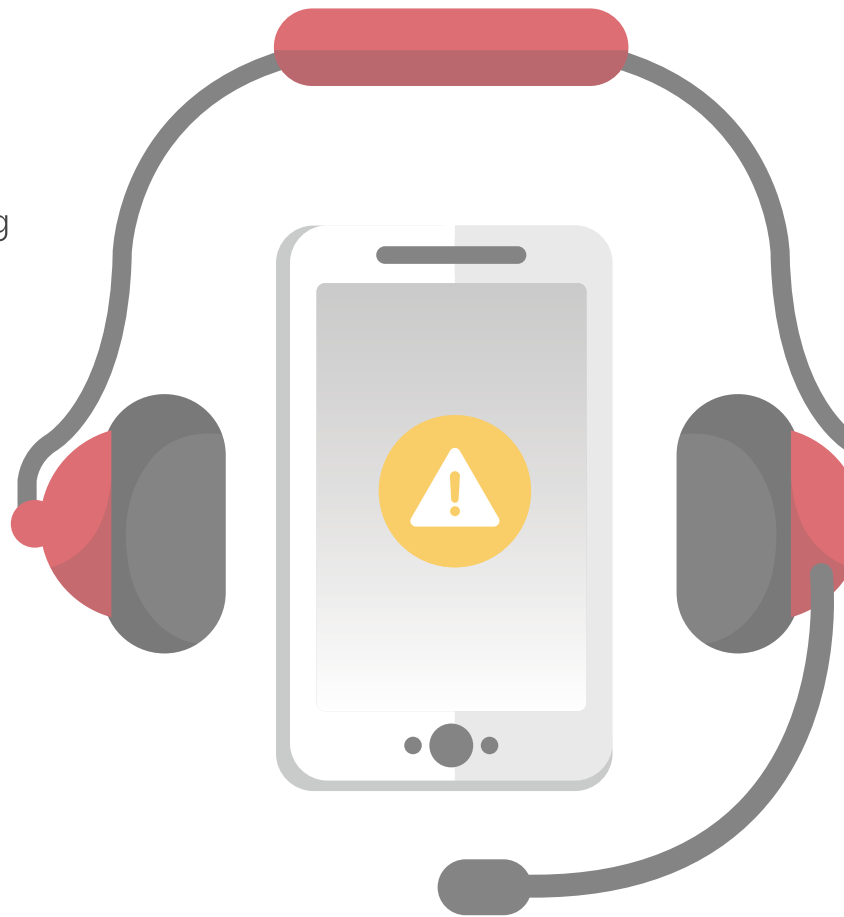
VISHING

How the Scam Happens

- » Imposters connect with individuals through telephone or social media as bankers/ company executives/ insurance agents/ government officials, etc., and seek confirmation of the secure credentials by sharing details like name or date of birth to gain confidence.
- » Imposters, then, pressurize or trick individuals into urgently sharing confidential details citing some emergency – block transaction, stop penalty, attractive discount, etc.
- » These credentials are then used to defraud the individuals.

Precautions

- » Bank officials/ financial institutions/ genuine entities never ask customers to share confidential information such as username/ password/ card details/ CVV/ OTP. Hence, never share the same with anyone.





S M S H I N G (SMS / Email / Instant Messaging / Call Scam)

How the Scam Happens

- » Fraudsters circulate fake messages in Instant messenger/ SMS /social media offering attractive loans, using name of bank / financing agency to gain confidence.
- » Fraudsters pressurize or trick individuals applying for loans into urgently sharing confidential details or directly demand various charges citing some emergency – block transaction, stop penalty, attractive discount, etc.
- » These confidential details are then used to defraud the customers.



Precautions

- » Never click on links received from unknown/unverified sources.
- » If you receive a code from the bank, even when you haven't requested for PIN change, or any other service, Report to corporatecenter@saraswatbank.com or call our 24*7 Toll Free no. **1800229999**.



SIM SWAP ATTACK

How the Scam Happens

- » Fraudster tries to gain access to individual's SIM card/ details of the SIM card as most of the account details & authentication is connected to the registered mobile number.
- » Using the SIM swap technique, the attacker gathers personal information by practices such as phishing, vishing, smishing, and more, to get a new sim card issued in the same individual's name.
- » Attacker uses this sim card, to conduct fraudulent transactions from the individual's bank accounts.

Precautions

- » Don't share any personal or confidential details with a stranger.
- » Never share the number mentioned on the reverse of your SIM card.
- » Be cautious while sharing your phone number on social media or any other website.
- » Never neglect any SMS sent by the mobile service operator regarding any SIM Swap request.
- » Check your bank account notification and statements regularly and report any inconsistent transaction or activity.





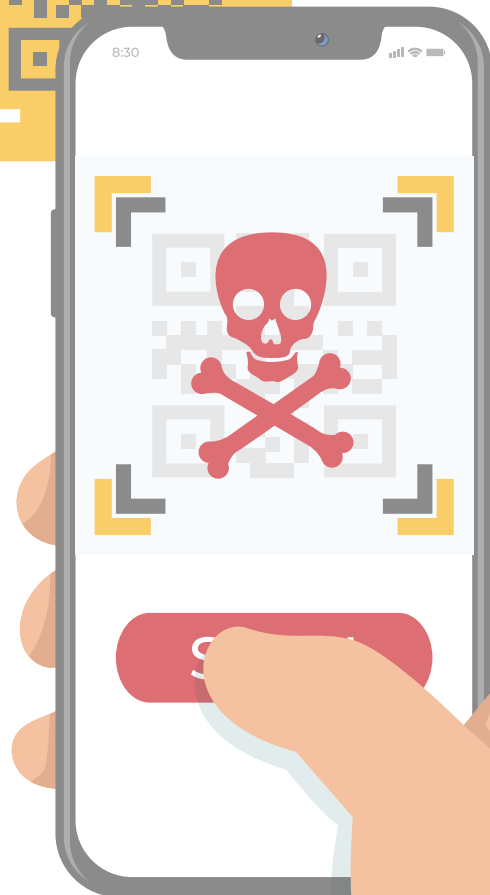
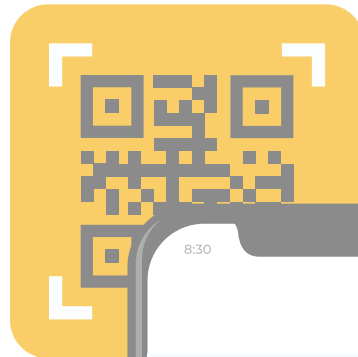
QR CODE FRAUDS

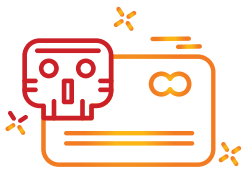
How the Scam Happens

- » Fraudster contacts individuals under some pretext like providing a refund or cashback.
- » Fraudster tricks individuals into scanning QR Code to receive a refund or cashback.
- » Fraudster withdraws money from customer's account.

Precautions

- » Be cautious while scanning any QR codes using payment apps. QR codes have embedded account details in them to transfer amounts to a particular account.
- » Scanning of QR codes if for payment of money and never for receiving money.
- » Enter your UPI PIN only in your UPI app while paying through trusted application.
- » Set pin / pattern / password / biometric lock to your UPI application & Never share your secret UPI PIN.





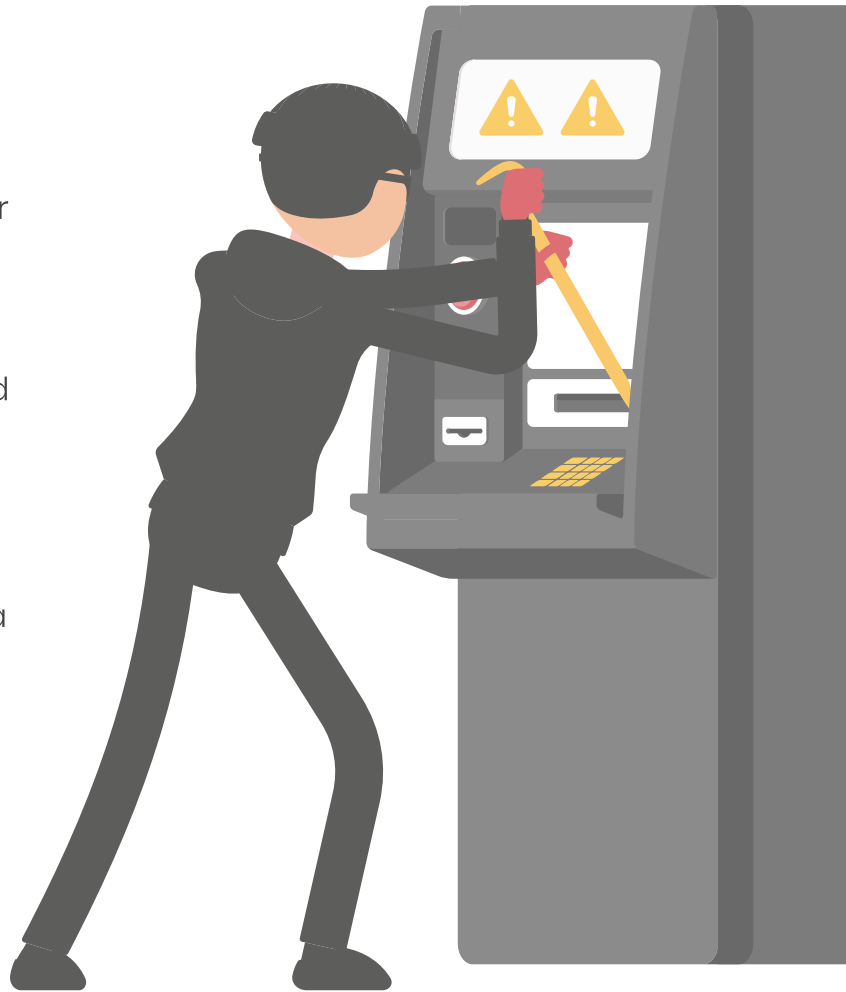
ATM CARD SKIMMING

How the Scam Happens

- » Fraudsters install skimming devices in ATM machines & steal data from individuals' card.
- » Fraudsters steal PINs by
 - Installing a dummy keypad or hiding a small pinhole camera near the keypad
 - Pretending to be another customer, the fraudster could stand behind the individual and gain access to your PIN as you enter it.
- » Fraudsters use this data to create a duplicate card and withdraw money from the individual's accounts.

Precautions

- » Verify that there is no extra device attached near card insertion slot or keypad of ATM machine while making a transaction.
- » Cover the keypad while entering PIN.
- » Never enter the PIN in presence of any other person standing close to you or share the card with anyone.





IMPERSONATING THROUGH SOCIAL MEDIA

How the Scam Happens

- » Fraudsters create fake account of a real individual on popular social media platforms like Facebook and Instagram. They send a request to individual's friends asking for money for urgent medical purposes, payments, etc.
- » Fraudsters also gain trust over a period of time and use the private information for extortion or blackmail later.

Precautions

- » Do not make payments to unknown person.
- » Do not share personal and confidential information on social media platforms.
- » Always verify genuineness of fund request with the friend / relative or confirm by a phone call / physical meeting to be sure that the profile is not impersonated.





FRAUDS USING ONLINE SELLING PLATFORMS

How the Scam Happens

- » Fraudsters pretend to be sellers on online platforms & sell latest products with attractive prices and luring offers.
- » When an individual pays online for such product, either no product is delivered or a different product is delivered like soap/a toothbrush which was never ordered.

Precautions

- » One should be careful while making financial transactions for online products.
- » Do not fall prey to limited offers or if the offer is too good to be true as it could be a scam.





FAKE LOAN WEBSITES/APP

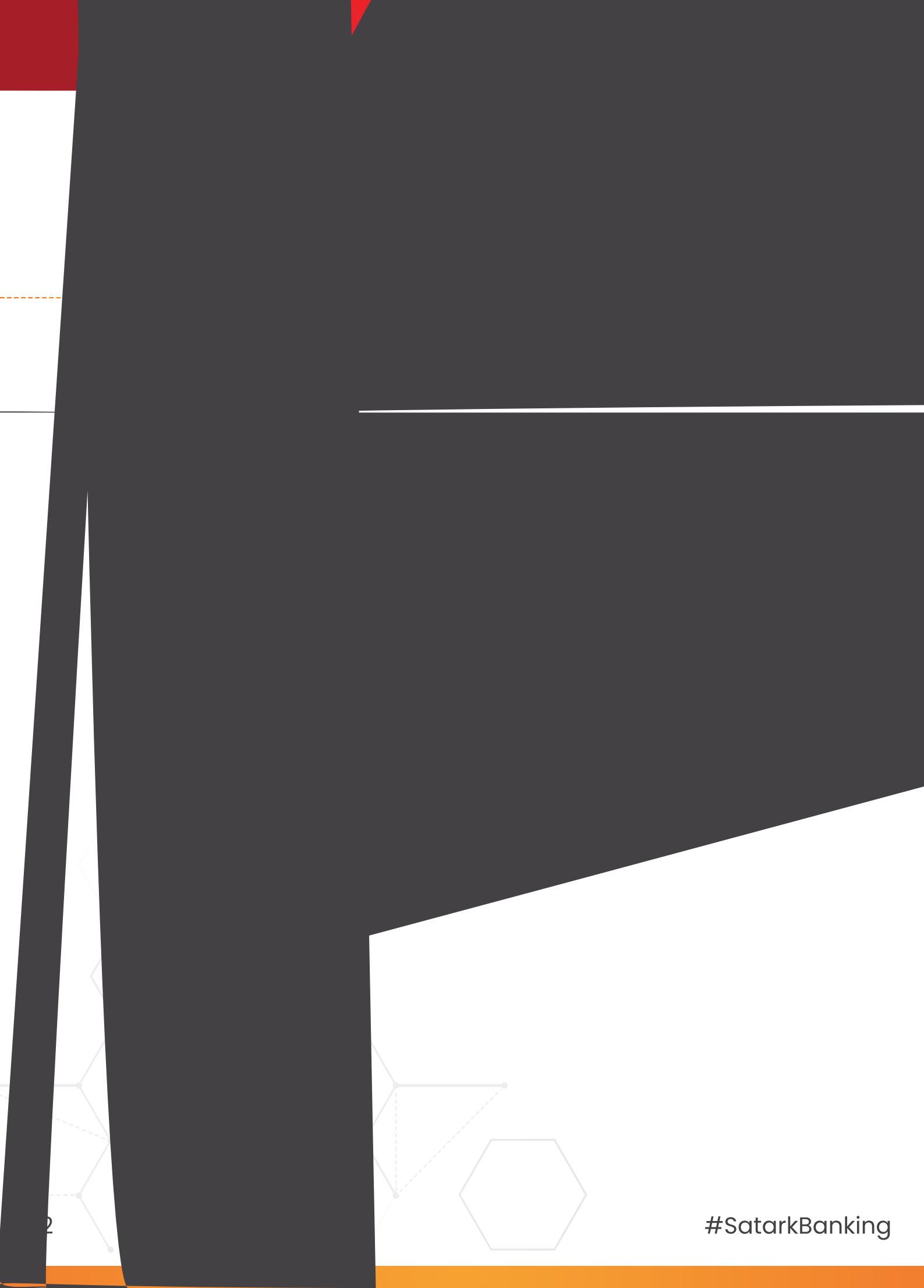
How the Scam Happens

- » Fraudsters advertise attractive Instant Loans offers for a limited period on unscrupulous Loan apps/websites.
- » Loan Seekers are asked to make urgent decisions using scareware tactics.
- » Loan seekers are asked their confidential personal information and duped with money/ significantly higher interest rates.

Precautions

- » Check for the authenticity of the money lender and money lending application.
- » Proceed with the loan application only after getting the genuine address & contact info.
- » Never make payments without processing your loan application.





#SatarkBanking



**Saraswat
Bank**

SATARK BANKING

— BE VIGILANT, BE SAFE —



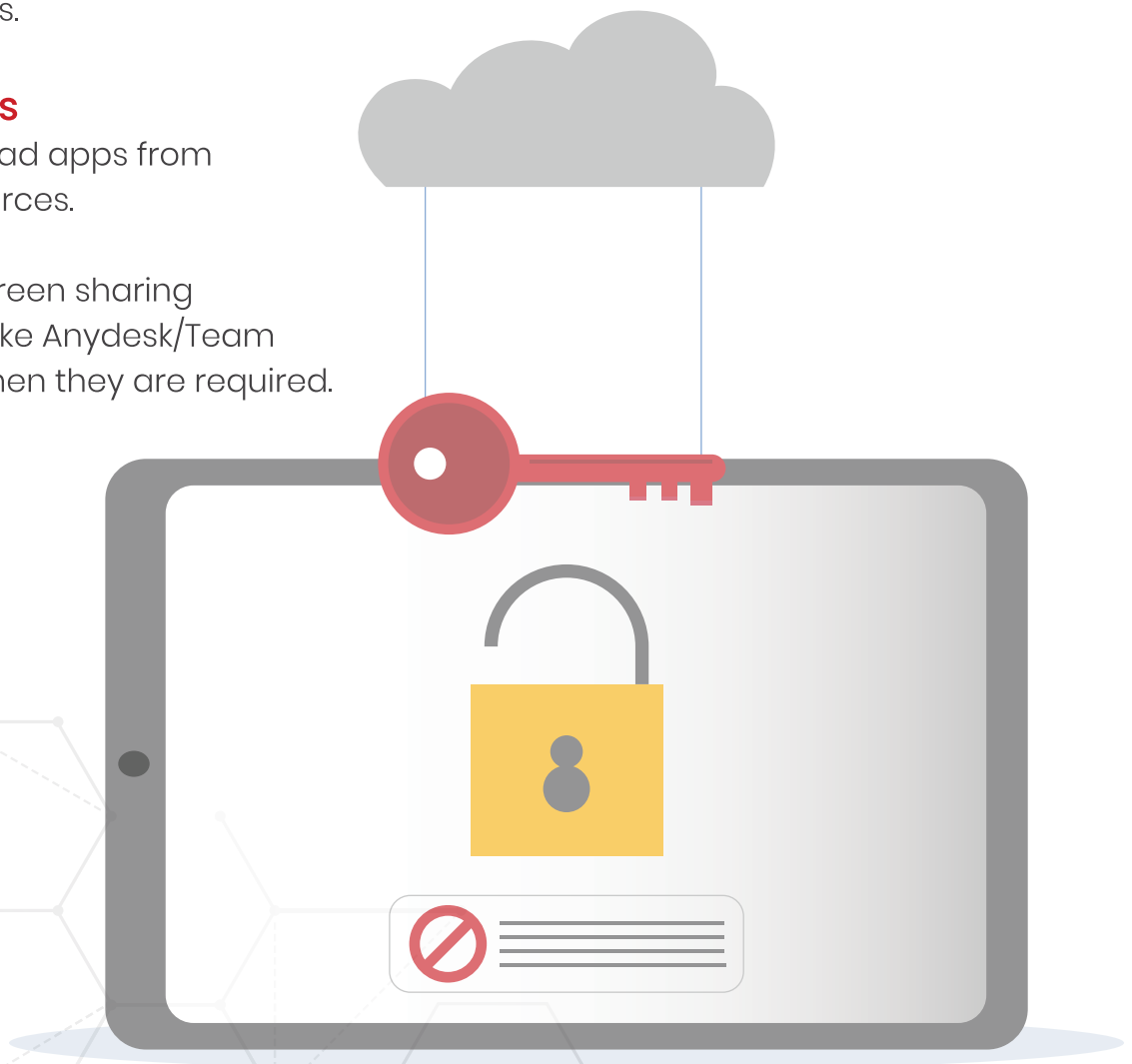
FRAUD BY REMOTE ACCESS

How the Scam Happens

- » Fraudsters trick an individual to download screen sharing apps through which they can watch / control your mobile / laptop to gain access to your financial credentials.
- » Later fraudsters make payments using your Internet banking / payment apps.

Precautions

- » Never download apps from unverified sources.
- » Only install screen sharing applications like Anydesk/Team Viewer etc. when they are required.





FRAUDULENT LOANS WITH FORGED DOCUMENTS

How the Scam Happens

- » Fraudsters pretend to be an NBFC/Bank employee to individuals seeking financial services and acquire KYC documents and other personal info like id cards, bank details, etc.
- » Fraudsters use this information to do identity theft and avail fraud loan/ benefits from a financial institution.

Precautions

- » Be vigilant while providing KYC and other personal documents including NACH form post, pre, or during the disbursement of loans from any entity.
- » Share personal documents only with the entity's authorized personnel or authorized email IDs of the entity.
- » Request purging of documents on non-sanction of loan or even post closure.





JUICE JACKING

How the Scam Happens

- » Attackers install malware into individuals' mobile phones when they charge mobile phones or any other smart device using compromised charging port of bus stop / railway station / airports, etc.
- » Attackers, then, gain access to sensitive data including contact details, emails, personal messages, photos, videos, and financial credentials.
- » These details are then used to carry out the fraudulent transactions by attackers.

Precautions

- » Avoid charging phones or other devices containing sensitive details at public charging points. Rather keep your devices fully charged before traveling or use personal power banks.
- » If unavoidable, charge the device via public charging points using the cable that can be used only as charging and not a data transfer cable.
- » You may also install an anti-virus solution that protects your smart device from malware and prevents data theft.





Be Vigilant, Be Safe



**Saraswat
Bank**

Saraswat Co-operative Bank Ltd.
(Scheduled Bank)