RAJARAMBAPU SAHA. BANK LTD., PETH.

E-Book on CYBER SECURITY AWARENESS

HAVE YOU BEEN

CHEATED ONLINE?

A GUIDE FOR VICTIMS OF

CYBERCRIME

#SmartBANKING

www.rajarambapubank.org

TABLE OF CONTENTS

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 Smart 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 / Mobile 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.
- Always set a password on your mobile device.
- Turn off your Wi-Fi, Bluetooth, GPS when not in use.

ATM Banking

- Change the PIN as you receive a new card from the bank.
- Don't write or share your PIN/CVV/OTP with any one.
- 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, click on such fake link and enters Credentials, this information is then available to The Phisher / Scammers.

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 Banker's / Company Executives / Insurance agent's / Government officials Seek confirmation of the secure credentials by Sharing details like Name or Date of Birth to Gain confidence.
- Imposters 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 Spam)

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 customercare@rajarambapubank.org or call on below Number. 24 * 7 call on. **9860600700**

SIM SWAP ATTACK

How the Scam Happens

Fraudsters tries to gain access to individuals 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 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 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.

RAJARAMBAPU SAHA. BANK LTD., PETH.

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 Machine & Steal data from individual's Card.

Fraudsters steal PIN's 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 at 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 & 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 exploitation, Blackmail later.

Precautions

Do not make payments to any Unknown person.

Do not share any 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

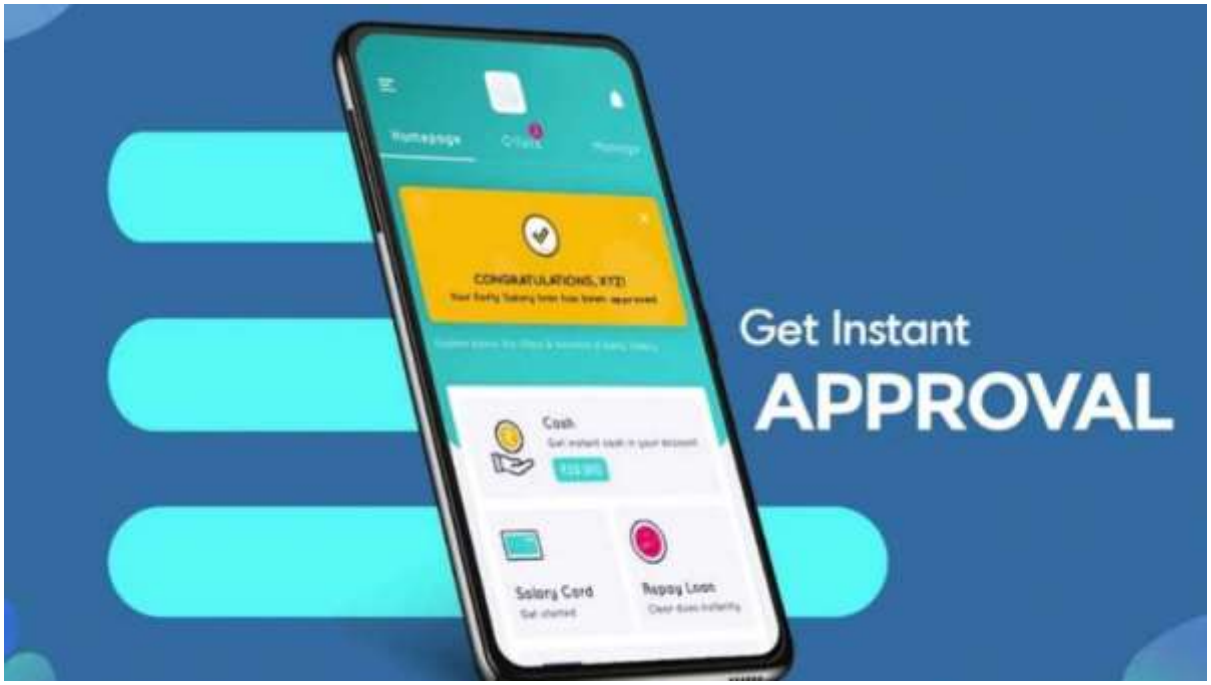
Fraudsters pretend to be sellers on online Platforms & sell latest products with Attractive prices and luring offers.

When an individual pays online for such Product either no product is delivered or A different product is delivered like Soap, 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.



F A K E L O A N W E B S I T E/A P P

How the Scam Happens

Fraudsters advertise attractive instant Loans offers for a Limited period on Unscrupulous Loan apps / website's.

Loan seekers are asked their confidential Personal information and duped with Money / Significantly higher interest rates.

Loan seekers are asked to make urgent Decisions using scareware tactics.

Precautions

Check for the authenticity of the money lender and money lending application.

Proceed with the loan application only after getting the genuine address and Contact information.

Never make payments without processing Your loan application.

MONEY MULE

How the Scam Happens

Fraudsters contact customers via emails, chat rooms, job websites or blogs, and convince them to receive money into their bank accounts, in exchange of attractive commissions.

The fraudsters then transfer the illegal Money into the money mule's account.

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.

Precautions

Do not respond to emails asking for your Bank account details. Never respond to Messages that promise lucrative Opportunities in the form of Jobs, lottery.

Always Monitor your Bank Account for any Suspicious withdrawals or Deposits.

For any overseas job offer, first confirm the identity and contact details of the Employing company

FRAUD BY REMOTE ACCESS

How the Scam Happens

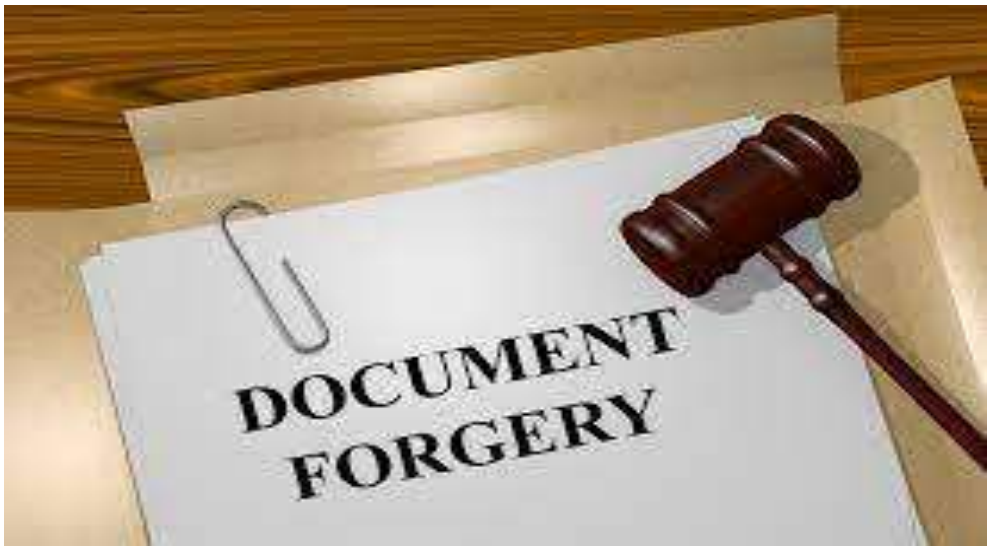
Fraudsters trick an individual to download Screen sharing apps through which they Can watch / control your Mobile / Laptop to Gain access to your financial credentials.

Later fraudsters make payments using your Internet / Mobile banking payments apps.

Precautions

Never Download apps from unverified Websites or sources.

Only install screen sharing applications Like Licensed TeamViewer / MS Teams 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 & acquire KYC documents & other Personal info like id Card, Bank details etc.

Fraudsters use this information to do identity Theft & avail fraud Loan / Benefits from a Financial institution.

Precautions

Be vigilant providing KYC & other Personal documents including NACH form Post, pre or during the Disbursement of Loans from Entity.

Share personal documents only with the Entity's authorized personnel or authorized Email ID's 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.

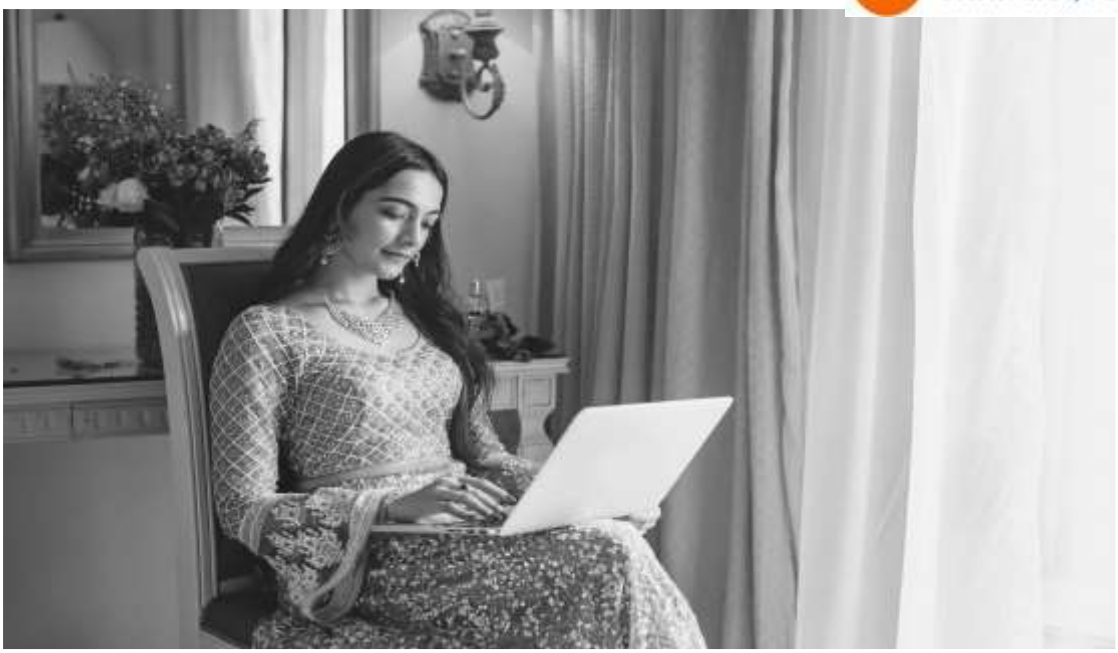
These details are then used to carry out The Fraudulent transactions by attackers.

Precautions

Avoid charging phones or other devices Containing sensitive details at public Charging points. Rather keep your devices Fully charged before travelling or use Personal power banks.

If unavailable 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.



MATRIMONY FRAUD

How the Scam Happens

Recent/new lucrative profile (5 –15 days old) highlighting income from job/business.

No social media details are shared, or if shared, the profile is recent with minimal friends.

They gain trust and convince the victim that no family members stay with them; hence, communication with family members is not possible.

Photographs show luxurious lifestyle – selfies in front of a bungalow, swimming pool, 5-star hotels, and malls wearing branded outfits, watches, and other accessories.

All communication happens on Audio or WhatsApp calls. If you insist on video calls, it happens outside the home/office – mostly in public places with lots of noise.

Precautions

Never trust a proposal without personal meetings/video calls with family members.

Insist on checking their social media accounts and friend lists. Also, do not forget to check friend list of friends.

Never send money even in case of a medical emergency, if you have not met the person.

Never accept any gifts without meeting in person.

Remember, custom officers never ask for online settlement without the formality of filling out forms.

SEXTORTION

This crime has been happening for the last 5-6 years. When smartphones grappled the market, everyone had smartphones, and video calls became common practice. In this crime, the target shares nude videos/photos, which are used by a fraudster, to blackmail the victim by making a threat to make it viral and share it with friends & relatives.

How to prevent this fraud?

- Never share high-resolution photos or videos on social media
- Never publicize your lonely/single status on social media
- Never use your real name and other details on apps like tinder
- Never respond to video calls from unknown numbers
- Never allow your intimate photos/videos to be captured by anyone
- In case you must attend a video call from an unknown number, ensure to cover the camera.

CYBERSECURITY

BE VIGILANT - BE SAFE