Be alert and practise safe banking

with

Banking Dhyaan Se

AXIS BANK

A customer service initiative by **Axis Bank**

Acknowledgement

This document has been created basis inputs 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

Digitization of banking system has crafted new corridors for customers to fulfil their financial needs with ease and speed. The current situation has also encouraged us to go digital as far as possible to minimize physical and social contact.

While we rejoice in the increased conveniences of digital banking, we are also more exposed to cybercrime and banking frauds. Most of the time, customers may be caught unaware, and may end up bearing a financial loss if they are not careful.

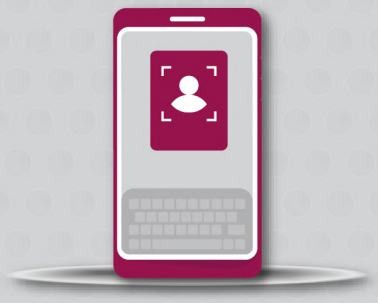
At Axis Bank, we care about you and are constantly looking at measures to help you safeguard your interest by sharing useful information from time to time.

This document is our initiative to create awareness and familiarize you with suspicious and fraudulent activities that are prevalent today. We have compiled some of the prominent fraudulent activities to help you understand how to identify such an activity, precautions that you need to take and how to report the same. Being cautious will enable you to minimize the chances of falling prey and incurring a financial loss.

We trust you will find this information useful and that you enjoy a safe and seamless banking experience, when you bank '*Dhyaan Se*.'

Stay safe!

Here are some general precautionary measures and good practices:



Avoid

- Visiting unsecured websites or using unknown browsers
- Saving passwords on public devices
- Accessing financial / confidential e-mails on public or free networks
- Clicking on suspicious looking pop ups, links and e-mails from unknown sources
- Storing secure credentials or passwords in e-mails or on unknown websites
- Sharing private information with unknown persons on social media
- Using same passwords for banking and other transactions
- Installing unknown applications or software
- Leaving your mobile or other electronic devices or apps unlocked

Never

- Share your PIN (Personal Identification Number), password, Credit or Debit Card numbers, CVV, copies of cheque book, KYC details with anyone
- Store sensitive or confidential information on unknown devices

Always

- Protect your phone with a strong screen password
- Use two-factor authentication wherever applicable / available
- Log out of the internet banking session immediately after usage
- Use the enable or disable feature and set-up transaction limits on your card or account based on your usage
- Verify the security of a website by looking for secured signs such as the padlock or https
- Use secure payment gateways for online payments
- Maintain strong passwords which would essentially be a combination of alphanumeric and special characters and change them regularly
- Use virtual keyboard on public devices since the keystrokes can also be captured through compromised devices, keyboard, etc.
- Install antivirus and anti-spyware on your devices, keep them up to date and install updates whenever available
- Scan any USB drives / storage devices before usage
- Protect your mobile apps with a password or conceal them from normal view using hidden space feature in mobile phones

#BankingDhyaanSe

About Online / Website frauds (1)

Modus Operandi
How can you be cautious & safe

Online Phishing

How it's done

- Fraudsters create a website which looks exactly like the Bank's genuine website
- These website links are circulated through SMS, social media, e-mail, etc.
- These links are masked to look like the authentic website and are designed to trick you into entering your credentials or sensitive and confidential information by just glancing at the link and not checking the detailed URL
- When you enter your credentials on these websites, the same is captured and misused by the fraudsters

Safety Tips

- Avoid unknown links even if they look authentic
- Verify the website details before entering financial credentials

Online Frauds

How it's done

- Fraudsters pretend to be legitimate buyers / sellers on online, ecommerce platforms
- They show interest in your product or trick you to buy from them by offering massive discounts or incentives
- Instead of making a payment, they lure you into completing the UPI 'request money' option to try and pull money from your bank account

Safety Tips

- Be careful while making financial transactions for online products
- You will never be asked to enter your PIN or password to receive money

#BankingDhyaanSe

About Online / Website frauds (2)

Modus Operandi
How can you be cautious & safe

Dubious Search Engine results

How it's done

- Fraudsters modify the customer care coordinates of companies and use Search Engine Optimisation (SEO) to push their fake number at the top of the search results on social media platforms
- While searching online for the customer care contact details of your Bank or other financial information / entities, you may accidentally contact such unverified / fake numbers, assuming them to be genuine
- You may end up sharing your personal or confidential and financial credentials and fall prey to fraud

Safety Tips

- Avoid searching for customer care contact details on search engine as they maybe camouflaged by fraudsters to lure victims
- Always look up official websites of banks / companies for their genuine contact details

Screen sharing / remote access

How it's done

- By tricking you into downloading screen sharing apps, fraudsters gain access to your personal data and financial credentials on your laptop / mobile devices and later make payments using your Banking and Payment apps

Safety Tips

- Do not download screen sharing apps recommended by any unknown persons
- Ensure you deactivate any screen sharing application before logging into any banking or financial app or website

#BankingDhyaanSe

About On Call / Mobile Frauds (1)

Modus Operandi
How can you be cautious & safe

Vishing calls

How it's done

- Imposter contacts customers via telephone call / social media posing as banking executives, etc. at times spoofing the toll free or customer care number of your bank
- The caller pressurizes and tries to convince the customer to share their confidential details or OTP citing various emergency reasons like immediate discontinuation of services, KYC non-compliance, closure of account / card, etc.
- They misuse these credentials to carry out fraudulent activities in your account

Safety Tips

- The Bank / any genuine entity will never ask you to share confidential information such as username, password, card details, PIN, CVV, OTP, etc.

Mobile app frauds

How it's done

- You are lured to download an unverified app on your mobile, laptop or desktop
- The links to these apps are shared and promoted via SMS, social media platforms, etc.
- They are malicious applications that allow fraudsters to gain complete access to your device

Safety Tips

- Never download application from unverified / unknown sources
- Delete SMS / e-mail received from unknown sources to avoid unintentionally clicking on the download link

#BankingDhyaanSe

About On Call / Mobile Frauds (2)

Modus Operandi
How can you be cautious & safe

OTP based Fraud

How it's done

- You may receive an SMS from a fraudster posing as the Bank offering loans or enhancement of credit limit and asking you to contact the number mentioned in the message
- When you call that number, you are asked to fill a few forms (even online) wherein your financial details are present making it easier for them to convince you to share OTP or PIN details, resulting in a financial loss

Safety Tips

- Never share your OTP, PIN or personal details in any form with anyone
- Check your SMS / e-mails regularly to ensure that no OTP is generated without your knowledge

Juice Jacking

How it's done

- Juice jacking is a type of cyber stealing, where, once your mobile is connected to any unknown / unverified charging ports, certain unknown apps / malware is installed on your device with which, the fraudsters can steal, control and access sensitive data, e-mail, SMS or saved passwords

Safety Tips

- Always avoid using public / unknown charging ports / cables

About On Call / Mobile Frauds (3)

Modus Operandi
How can you be cautious & safe

SIM Swap frauds

How it's done

- Your account details and authentication are connected to your registered mobile number. Fraudsters try to gain access to the OTP and alerts required to carry out financial transactions by obtaining a new replacement SIM card for your number
- The fraudster visits your mobile operator's retail outlet posing as yourself with a fake ID proof to get your original SIM blocked and collect a new SIM with your mobile number
- Alternatively, they scare or trick you into upgrading your SIM card by sending an SMS shared by them with your operator which deactivates your SIM and activates the SIM card with your mobile number in their possession

Safety Tips

- Beware of social engineering scams aimed at stealing your confidential and personal data
- If your mobile phone suddenly does not show any network connectivity, enquire with your mobile service provider immediately about the status of your service to ensure that no duplicate SIM is being issued for your SIM

About Other Types of Frauds (1)

Modus Operandi
How can you be cautious & safe

Frauds through social media

How it's done

- Fraudsters impersonate you and create fake accounts on popular social media platforms
- When your unlocked phone is inadvertently handed over (for making an emergency call or for repair) or lying unattended, the fraudster is able to receive the OTP sent to your mobile to access your profile and generate desktop version of certain applications giving them access to your contacts, online profile and chat messages
- They send requests to your friends asking for money for urgent medical help, etc.

Safety Tips

- Verify the authenticity of the request by reaching out to your contacts by phone or in person before making any payment
- Never leave your phone unattended without being locked

QR scan-based frauds

How it's done

- Fraudsters may contact you under various pretexts and lure you into scanning QR codes using payment apps and completing the payment process
- These QR codes have predefined account details to transfer amount to any specified account which the fraudster camouflages to trick you into completing the money transfer from your account

Safety Tips

- Be cautious while scanning any QR codes using payment apps

About Other Types of Frauds (2)

Modus Operandi
How can you be cautious & safe

Lottery or Job Fraud scams

How it's done

- Fraudsters send e-mail or make phone calls informing you have just won a huge lottery / prize or pose as the official of a reputed company with a job offering
- However, in order to receive the money / gift or complete the selection process, you may be asked to pay some money upfront
- As the amount requested is usually a very small percentage of the lottery / prize or considered critical to secure the job, you may end up making such a payment

Safety Tips

- Do not make payments or share your secure credentials for any lottery calls / e-mails
- Always question the authenticity of any unbelievable lottery or offers
- Remember, any genuine company offering a job would never ask for money

ATM card skimming

How it's done

- Fraudsters install skimming devices in ATM machines to steal data, create a duplicate card and withdraw money from your account
- They may also install dummy keypads or tiny cameras to capture information entered by you
- They can also pose as a customer using the ATM services to view your PIN, while you enter it or offer to help you complete your transaction, in case you are unable to withdraw cash

Safety Tips

- Be vigilant and ensure that there is no extra device attached near the card insertion slot or keypad of the ATM machine
- DO NOT enter card details in the presence of anyone standing close to you
- Cover the keypad while entering the PIN and do not share your card or PIN with anyone
- Exit the ATM premises immediately if you feel anything suspicious

#BankingDhyaanSe

Report a suspicious or fraudulent transaction to Axis Bank

In case you come across a suspicious transaction or have made a fraudulent transaction, you can reach out to the channels mentioned below:

- Call our Phone Banking numbers: 1860 419 5555 / 1860 500 5555
- Write to us at https://www.axisbank.com/support/
- Visit any Axis Bank branch

Thank you for your time and attention.

#BankingDhyaanSe