Scammers here,
Scammers there,
Don't get trapped anywhere!

#BankingDhyaanSe 2.0

AXIS BANK

You work hard to earn, why not keep your earnings safe?

Welcome to the **Axis Bank Fraud Awareness Booklet #BankingDhyaanSe 2.0,** your key to understanding and preventing financial scams. In a rapidly evolving digital age, knowledge is your shield against fraudsters. This guidebook provides you with insights, real-life examples, and practical tips to protect your hard-earned money.

As your trusted partner in banking, Axis Bank is dedicated to helping you navigate the digital landscape confidently. Let's guard against deception and secure a brighter financial future together.

OTP Scams

One-Time Password is a golden key to access your impenetrable digital kingdom.

To keep out the cunning tricksters from stealing your precious key, you have to be the guard of your fortress!

Keep OTPs confidential: Never share OTPs with anyone through phone calls, e-mails, text messages, or social media and stay vigilant like a watchful guard.

Verify requests: Trust but verify. If an OTP request pops up out of the blue or feels fishy, don't rush. Double-check its authenticity before you react.

Use official websites or apps: Stay safe when sharing OTPs. Always visit the official site or app directly - no shortcuts. Typing beats clicking links any day.

Be cautious of urgent requests: Scammers often create a sense of urgency to pressurize you into sharing your OTP. Take a step back, think critically, and verify the request independently before acting.

Enable two-factor authentication: Double down on security with 2FA (Two-Factor Authentication). Choose rock-solid options like app-based or hardware tokens. They outshine SMS OTPs any day.

Please remember, Bank will not ask for your CVV, OTP, PIN, Card Number, Passwords, etc. Do not share these details with anyone.

Credit Card Scams

Let's imagine Credit Card scams as a sneaky game of hide and seek. Just like how a scammer tries to hide their true intentions, they might trick you into revealing your Credit Card information.

To avoid falling into their trap, keep these tips in mind:

Watch out for phishers: Scammers might pretend to be from your bank or a familiar company. Don't fall for their tricks; verify their identity.

Check your statements: Regularly review your Credit Card Statements. If you spot unfamiliar spends or charges, it's like discovering hidden players in the game-address them immediately.

Set transaction limits: Set transaction limits on all your payment channels and customize the 'Manage Usage' section, as per your requirement.

Secure sites only: When shopping online, make sure the website is secure (look for "https" in the URL). It's like choosing a safe playground for the game.

Stay updated: Keep an eye on the latest scam tactics, just like you learn new strategies in the game. This way, you'll be prepared to outsmart the scammers.

Electricity Bill Frauds

How to identify a fake SMS?

Picture this: You're enjoying a relaxing evening at home, binge-watching your favourite show, when your phone buzzes with an incoming message. It's your electricity provider, and they're claiming you owe an exorbitant amount for your latest bill.

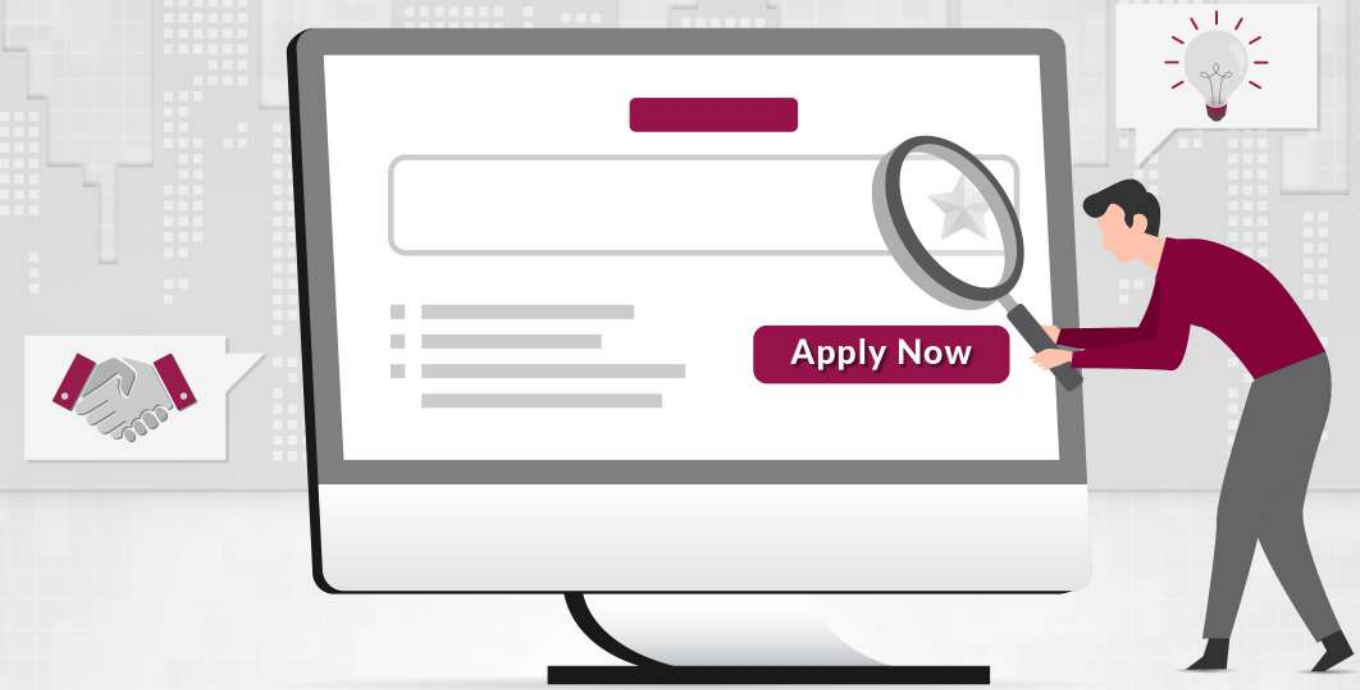
Before you panic, consider this: Electricity bill fraud, much like a stealthy phantom, can creep into your life without warning.

Never share your confidential details with anyone or click on unsolicited links.

Use only official and secured websites to make bill payments.

Remember, the electricity department never asks for personal details or payments through random / unregistered numbers.

Job Scams



Imagine you're scrolling through job listings, and suddenly you stumble upon a job offer that seems too good to be true. Unlimited vacation days, work in your pajamas, and a six-figure salary for data entry? Sign me up!

Wait, before you hit that "Apply Now" button!

Research the company: Look up the company online and ensure it's reputable. Scammers often create fake companies with convincing websites.

Don't pay upfront: Legitimate employers won't ask you to pay for training, materials, or background checks before you start working.

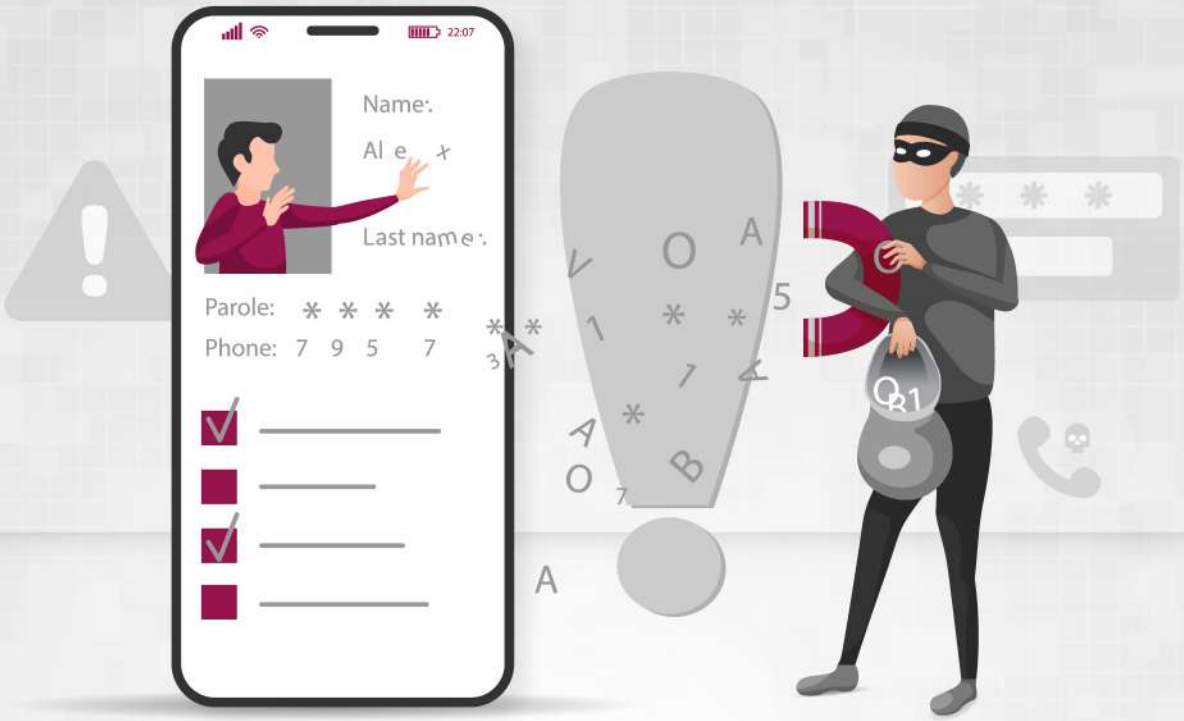
Watch for red flags: Be wary if the job requires you to provide sensitive information like your Social Security number or financial details right away.

Too quick to hire: If you're offered a job on the spot without an interview or much information exchanged, it could be a scam.

Trust your instincts: If something feels off, trust your gut and proceed with caution or walk away.

Remember, safeguarding your personal and financial information when job hunting should be your first priority.

Call Spoofing Scams



Just like how a magician can make things appear different from what they actually are, scammers can manipulate your Caller ID to make it seem like they're someone you know or trust – in this case, your Bank. It's like a digital disguise for their true identity.

To protect yourself from this sneaky trick, remember these tips:

Verify with Caution: Even if the caller ID looks familiar, stay skeptical. If someone asks for sensitive information, double-check their identity through other means.

Don't Share Personal Info: Never give out personal or financial information over the phone, even if the caller seems legitimate. Hang up and call back using a trusted number.

Stay Private: Be cautious about what personal details you share online or on social media. Scammers often gather information from these sources to make their spoofed calls more convincing.

Use Call Blocking: Explore call-blocking apps or features provided by your phone carrier. They can help filter out potential scam calls.

Do not search for phone numbers on Google or any search engine. If you do so, do not click on any links sent to you by the entity or merchant.

Additionally, please ensure that you have the latest versions of the banking applications downloaded on your devices from only the authorised application stores.
Please check this periodically.

Remember, just like you wouldn't trust a masked stranger in real life, don't trust a masked caller on the phone. Stay vigilant!

UPI Refund Scams

Imagine you're scrolling through your phone when you spot a UPI refund notification, and suddenly, you're on cloud nine! But wait. This could be a UPI Refund Scam!

UPI or The Unified Payments Interface has become a part of our daily life. From paying at your local kirana stores to recharging phones to booking flight tickets, we use UPI payment for various things. So scamsters have started adopting new methods to trick people using UPI apps.

Never fall for their official jargon and professional language. Keep in mind the following tips:

Beware of links: Scammers may send you a link, urging you to register to claim a refund.

High-pressure tactics: They'll pressure you to fill in bank details or UPI PIN immediately for instant money.

Verify eligibility: Ensure you're eligible for a refund. If yes, check for a trusted source.

Remember, Bank or other officials will never ask you for such sensitive details.

Phishing Scams

Imagine you're a fish swimming peacefully in a clear pond, minding your own business. Suddenly, a shiny, tempting bait dangles in front of you. You're intrigued but wait – something's fishy!

This is exactly what happens in the digital realm with phishing scams.

Cybercriminals pose as trustworthy figures to trick you into revealing sensitive information, just like a fish gets lured by bait. They send fake emails, messages, or websites that seem legit, often imitating banks, social media, or even your boss.

To dodge these digital hooks, remember these tips:

- **Double-check URLs:** Hover over links to see where they truly lead.
- **Don't share personal info:** Legit entities won't ask for sensitive stuff via email.
- **Stay suspicious:** Unexpected requests? Verify through other means before acting.
- **Update security software:** Keep your digital pond guarded with the latest defenses.

Just like a wary fish, be cautious and swim smartly in the vast ocean of the internet!

Vishing Scams

Your phone rings, and it's your so-called bank with an 'urgent' call claiming your account is compromised, or maybe the 'winning' call claiming it's your lucky day, and you've won a surprise!

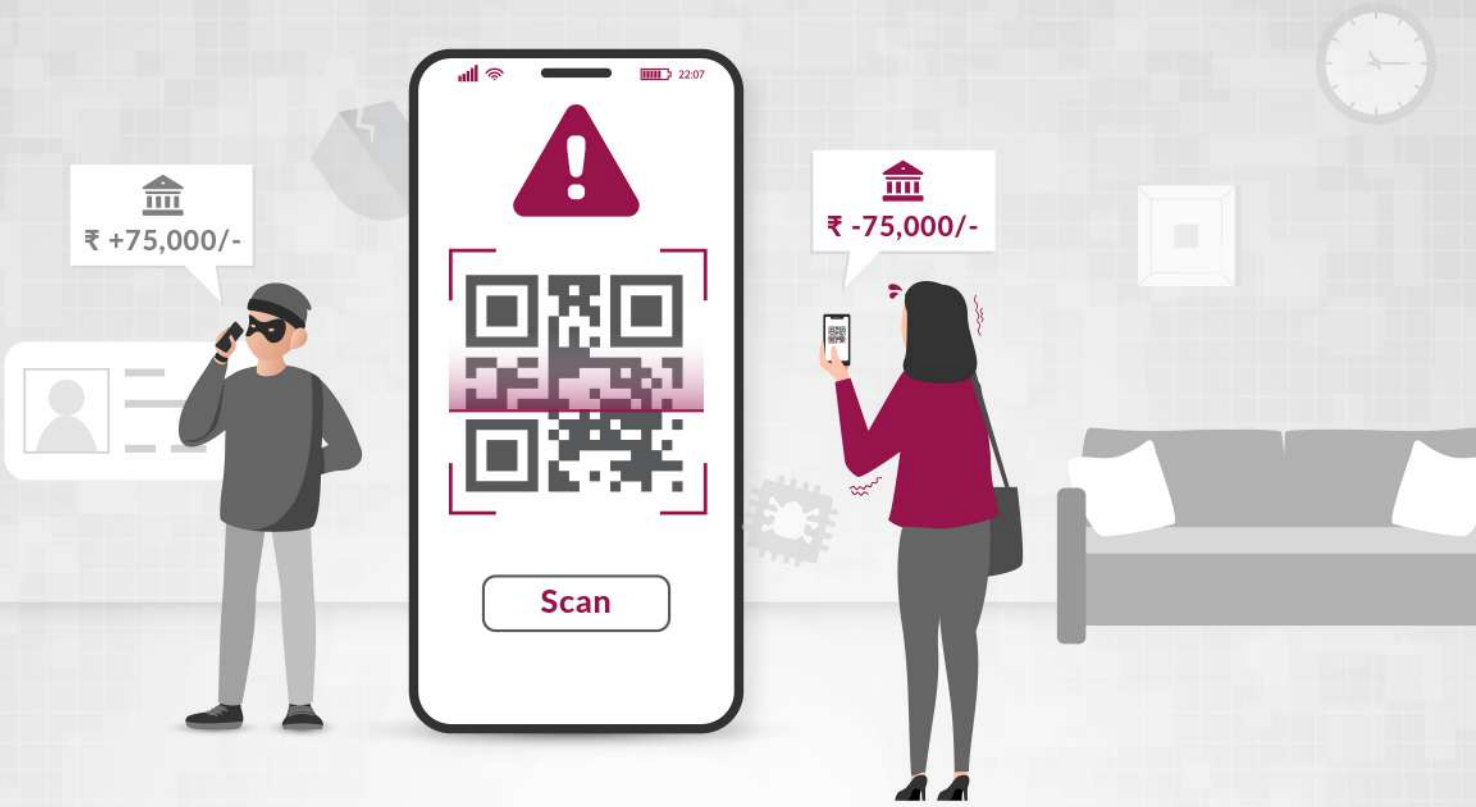
Hold the phone (literally)!

To stay safe from such scams, remember the following tips:

- Never spill your personal details over the phone.
- Be Sherlock Holmes and verify that caller's identity.
- Don't fall for the drama! Stay cool when they turn up the heat.

Remember to be careful about sharing info with strangers online – stay smart to keep your stuff safe!

UPI Scams – Request Money option



Sneha advertised her furniture on an online buying and selling app. A buyer, claiming to be a paramilitary personnel, sent a QR code for payment on WhatsApp. Sneha scanned it and lost ₹ 75,000.

Does this sound familiar? Are you afraid of falling prey to UPI Fraud due to your frequent usage of UPI payment platforms?

Always remember:

- UPI PIN is required only to make a payment and not to receive any payment.
- Do not share your OTP, UPI PIN or any confidential details with anyone.
- Stop, the moment your UPI PIN is asked to receive a payment! This may actually be a payment request and not a collect request.
- Always verify the mobile number and name in the UPI application before initiating any payment.

QR Code Scan Fraud

- Scan QR codes on payment apps with caution; they contain account details for money transfers.
- Don't scan QR codes to receive money; scanning barcodes / QR codes or entering mobile banking PIN (m-PIN), passwords, etc. is unnecessary in transactions for receiving funds.

Buyer / seller showing unreasonable haste or urgency is most likely a fraudster. Remain calm, always seek clarification and ask necessary questions.

Unverified Mobile App Frauds

You receive an SMS, an email, or even a message from a long-lost cousin you never knew existed, all with a link that looks like a legit app from your favorite authorized entity.

Hold on a minute! These aren't friendly downloads; they're invitations to a digital party you definitely don't want to attend!

Scammers send fake app links via SMS, email, or social media that look like legitimate ones. They persuade users to click on them, leading to the download of unknown apps. Once installed, scammers gain access to the device, including confidential information and OTPs.

- Avoid downloading apps from unknown sources or at the request of strangers.
- Verify app publishers and user ratings before downloading.
- Review permissions and app requests (e.g. contacts, photos) and grant only necessary ones.

Remember, Bank or other officials will never ask you for such sensitive details.

ATM Card Skimming Fraud

Think of ATM skimming like a digital pickpocketing. While you use an ATM to withdraw money or check your balance, fraudsters set up hidden devices on the machine to record your card information. These devices can be as inconspicuous as a fake card slot or a tiny camera.

Inspect the ATM: Always check the card slot and keypad for any unusual attachments, loose parts, or hidden cameras before using an ATM.

Cover your PIN: Shield your PIN entry with your hand or body, making it hard for cameras or onlookers to see.

Regularly check statements: Keep an eye on your bank statements and transactions. Report any unfamiliar activity to your bank immediately.

Beware of calls: If someone claiming to be from your bank calls and asks for sensitive information, be cautious. Banks rarely ask for PINs or full card numbers over the phone.

Use secure ATMs: Opt for ATMs in well-lit areas or those attached to bank branches, as they are less likely to be tampered with.

Stay updated: Stay informed about the latest scams and fraud tactics to better protect yourself.

Remember, staying vigilant and following these tips can help you avoid falling victim to ATM card skimming fraud and keep your finances safe.

Remote Access Fraud

Scammers lure customers into downloading a screen-sharing app. With it, they sneak into your device, spy on you, and swipe your financial info. Then, they go shopping with your money!

To steer clear of such scams, remember these tips:

Verify callers: Always double-check the identity of the caller by independently looking up the official contact information of the organization they claim to represent.

No rush decisions: Don't make impulsive decisions under pressure. Take your time to think and verify before granting access or sharing sensitive information.

Secure your devices: Keep your devices updated with the latest security patches and use strong, unique passwords for each account.

Educate yourself: Learn about common scams and tactics so you can recognize them when they occur.

Guard personal information: Be cautious about sharing personal or financial details over the phone, email, or online unless you're sure about the legitimacy of the request.

Be vigilant to keep the virtual door locked against remote access fraudsters trying to sneak into your digital life.

Please Note - In case you notice a black / blank screen, please do not proceed with any actionable on your system. This might be a sign that your screen might be visible to others.

SIM Swap Fraud

Imagine scammers pulling off a phone heist! They pretend to be you, saying they lost their SIM card, and bam—they've got your number. With that, they crash into your online accounts, like your bank or email, and stir up chaos!

Stop the swap Scam! Remember the following tips.

- Don't share SIM card identity details.
- Monitor your phone's network access.
- If there is no network for a while, contact your operator to check for duplicate SIMs.

Be vigilant to keep the virtual door locked against remote access fraudsters trying to sneak into your digital life.

How to report a Fraudulent Transaction?

Visit **www.axisbank.com** > Support > Scroll down to 'Reach us here' section > Speak with us > Select 'Report a fraud or Dispute' > Report a Fraud > Choose relevant option from the drop-down list of your Query > Click on Call

To file a complaint with RBI, visit https://cms.rbi.org.in

Call the Toll-free number 14448 (Monday to Friday, 9:30 a.m. to 5:15 p.m., Excluding National Holidays).

Send a physical complaint: Letter / post to 'Centralized Receipt and Processing Centre, 4th Floor, Reserve Bank of India, Sector -17, Central Vista, Chandigarh – 160 017'. **Please visit** https://cms.rbi.org.in for more details on the required format.

To report a Cyber Crime, dial helpline number **155260** or **1930** or report the incident on National Cybercrime Reporting Portal **(www.cybercrime.gov.in).**