Simplifying your Digital Life

Making Life Easy

- Moving into digital world the right option
- Cashless the right way to go forward
- Covid era – More of contactless transactions
- At the comfort of home
- No standing in long queues
- More transparency in transactions
- Cost effective

Use of Digital Platforms

- Bill Payments/Recharges
- Investments
- Electricity Payments
- Tax Payments
- Fund Transfer
- Contactless Payments
- Online Purchase –Food, Grocery, Merchandise

Modes Available

- DEBIT CARD
- CREDIT CARD
- MOBILE BANKING
- INTERNET BANKING
- QR CODES
- WALLETS
- THIRD PARTY APPS/UPI

Reward Points

Credit Cards

- Reward Points program are allotted on successful merchant transactions after settlement of funds.

- Reward point is not available for
  - Cash withdrawals from ATMs/ Cash at POS
  - Purchase of fuel at fuel stations
  - Purchase of jewellery
- 1 reward point = Rs. 0.25
- Cardholder will earn
  - 1 reward point for every Rs. 100 spent using Gold variant.
  - 2 reward point for every Rs. 100 spent using Platinum variant.
  - 4 reward point for every Rs. 100 spent using Signature/Select variant
  - Credit Card Points Valid for 12 months.

Points Can be redeemed at –

- Union Rewardz (available at App Store and Google Play Store App for redemption of points accumulated)
- **https://unionrewardz.com**
- Minimum reward point from redemption in Credit Card is Gold 500 Platinum 750 and Signature /Select 1000

Debit Cards

Classic, Gold, Platinum Debit cards - 1 reward point/₹100 spent

Signature Debit card - 4 reward point/₹100 spent

1 reward point = Rs. 0.25, valid for 36 months

Risk Cover and benefits available under various Insurance Schemes : Life and General Insurance (Accidental Death)

Risk cover for the same event under multiple insurance policies.

Accidental Death Insurance Cover

1. **PMSBY** – Pradhan Mantri Suraksha Bima Yojana accidental death cover at subsidized premium is available through Govt, of India Scheme PMSBY.

Eligibility -18 to 70 Years. Period June 1-May 31st. Premium: Rs. 12 per annum

Risk Cover- Accidental Death- Rs 2 Lakh. Injury due to accident-Rs 1 to Rs 2 Lakh.

Even if the account holder is having multiple accounts with the same Bank/Different Bank, Risk is covered per policy holder only. (Max –Rs 2 Lakh)

2. **RuPay Debit Cards** **-** Risk benefit per Customer. Even if a person is having different RuPay cards, risk can be covered per person only. The Insurance policy is applicable for the compensation of only one eligible RuPay card per cardholder or per customer, even if multiple cards held by cardholder of same / different banks meet the eligibility criteria. The choice of the card for the claim would rest with the customer.

3. **Visa /Master Debit/Credit Cards** **-** Accidental Death -Covers Risk per Bank/per Customer, subject to conditions. In respect of Accidental Death of a person, for the same person claims can be made for all the above categories.

4. In case of death happened due to Train/ Flight accident compensation can be claimed as per the Insurance cover available in respective Tickets. This is apart from any compensation sanctioned by respective Govt/Airlines,

5. In case of accidental death on roads involving Motor Vehicles, claim can be made under Motor Vehicle Insurance Act. Compensation will be decided by the court based on the age, income and dependents of the insured.

6. Apart from the above in case of death due to natural calamity, freak accidents State Government sanction compensation through Chief Minister Relief Fund.

This cover is available through specific insurance schemes of the GIC, Banks or GOI Subsidized Scheme. In addition, debit (ATM Cards) and credit cards of the Banks have the in-built cover for accidental death. (In fact, many debit cards have certain unknown additional features as accidental death risk coverage, free access to airport lounge, baggage insurance, buyers' protection subject to conditions.)

Digital Safeguarding

1. The remote access mobile application scam

Modus operandi

Fraudsters, who had listed fake numbers online under an NGO's name, gained access to a Mumbai resident's debit card details by asking software tool, which provides a third party a complete view of the user transfer funds to the NGO to cremate her pet. Instead, her debit card details were compromised and Rs 30,000 was withdrawn from her bank account.

Lessons to learn

Do not seek help from strangers to complete payment transactions. Do not download apps, except official ones, recommended by seemingly-helpful people, even if they claim to be bank staff.

2. Trap for gullible insurance seekers

Modus operandi

In this, scammers prey on an individual's inability to spot the difference between the official and fake portals of the insurance regulator. A counterfeit portal going by the URL www.irdaionline.org managed to sell fake policies to insurance seekers until the IRDAI issued an alert, and the URL was blocked.

Lessons to learn

Stay away from portals misusing domains that are akin to regulators' official ones to swindle funds.

3. Phishing SMS's promising income tax refund Modus operandi

Modus operandi

A Mumbai-based private sector employee received a link, purportedly from the income tax department, regarding a tax refund he was eligible for. Once he clicked on the link, he was directed to a mobile application that got downloaded on his phone. Tricksters elicited his account access details and siphoned off money.

Lessons to learn

The income tax department directly credits the refund to the bank account mentioned in your IT return form. Do not trust any messages, links, online forms or calls seeking additional account/card details.

4. The KYC update hoax

Modus operandi

An IAS officer in Udaipur lost Rs 6 lakh when she clicked on a fraudulent link asking her to update her KYC. She was prompted to enter her account details and the OTP received, following which she received messages from her bank notifying her of debits worth Rs 6 lakh.

Lessons to learn

Do not click on links received through SMS's. complete the process, if required.

5. Fake UPI-based payment links

Modus operandi

Fraudster asked the victim, a Pune-based trader, to transfer a nominal amount of Rs 10 to a mobile number from his digital wallet. It was presented as 'registration fee' to initiate the online purchase of a scooter. Subsequently, he received payment links where he had to enter his UPI ID and OTP received and send it back to the fraudster. The information was used to transfer Rs 1.53 lakh out of his accounts.

Lessons to learn

Transact only through the official BHIM or bank UPI apps. Do not use links sent by unknown entities, even if they seem authentic.

6. Fraudulent NPCI/UPI/BHIM handles and portals Modus operandi

Modus operandi

Myriad Twitter handles masquerading as @NPCI_BHIM official helpline handle have mushroomed on the micro-blogging site. The fake accounts trick customers looking for help to reveal their account, wallet or card details.

Lessons to learn

Look for verified-by-twitter blue ticks while interacting with National Payments Corporation of India (NPCI), bank or payment wallet help lines.

7. Lack of awareness of UPI pay options

Modus operandi

A Pune resident who wished to sell his air-cooler was tricked by a prospective buyer who agreed to pay Rs 9,000 through a UPI-based app. However, the latter sent a 'pay' request to the former who promptly authorized it without realizing that the amount would be debited from, not credited to, his account.

Lessons to learn

Use of newer technologies calls for additional caution. Since UPI-based apps enable push (pay/send) and pull (receive/collect) transactions, newer users could get confused. Understand the processes thoroughly before rushing to use them.

Do's and Don't's of Internet Banking

Do's	Don'ts
Always type the address of the bank's website in the address bar of the browser.	Do not provide any information on a pop-up window however officially looking or appealing it may be.
Always check the last login date and time in the post login page.	Do not let your computer remember your password. Never accept auto complete option provided by your computer/ browser,
Use best practices for creating strong passwords (alphanumeric password)	Do not leave your internet banking session unattended. Always logout completely.
Change your passwords frequently.	Never share / communicate / respond your Internet Banking credentials to anyone.
Use the virtual keyboard to prevent key-logger compromises as such malware can track keystrokes in a physical keyboard.	Do not store passwords in a file on any device including mobile or similar devices.
Bank will never send e-mails, SMS or make calls asking for personal information.	
❖ Mobile numbers not to be changed frequently ❖ Always update the mobile banking Application to its latest version ❖ Customer to download apps from trusted sources or a legitimate app store. ❖ Always lock mobile phone to prevent unauthorized users from gaining access to personal and M Banking Apps	❖ Should not disclose login PIN and transaction PIN ❖ Never open attachments or download apps from unknown sources on your mobile phone. ❖ Never connect your mobile phones to unsecure Wi-Fi connections available at public places.

Cyber security Best Practices

1. Create passwords and make them strong

A strong password is at least 12 characters long. Strong password tips include the use a mix of letters, numbers and symbols, and try not to include personal information.

2. Think before you act

Emails and communication that create a sense of urgency such as a problem with your bank account or tax is likely a scam. Consider reaching out directly to the company by phone to determine if the email is legitimate or not.

3. When in doubt, throw it out

Clicking on links in emails is often how scammers get access to personal information. If an email looks unusual, even if you know the person who sent it, it's best to delete it.

4. Share with care

Be aware of what you share publicly on social media sites like Facebook.

5. Use security software

Install security software on your devices from a reliable source and keep it updated. It is best to run the anti-virus software regularly.

6. Log out

Remember to log out of apps and websites when you are done using them. Leaving them open on your computer screen could make you vulnerable to security and privacy risks.

7. Consider support

If you live alone or spend a lot of time by yourself, consider a trusted source to serve as a second set of eyes and ears. Adult family members and grandchildren who are computer savvy may be willing to help.

Steps to prevent Financial Frauds.

If anyone asks for OTP, do not respond.

A new type of Cyber Fraud has been initiated by Fraudsters. In such frauds, customers get calls from fraudsters asking to share the OTP so received in order to postpone their loan RMIs. If the OTP is shared, the amount is immediately siphoned away by fraudsters.

FRAUDS USING ONLINE SELLING PLATFORMS

Modus Operandi:

- ➢ Fraudsters posing as buyer shows interest in your product.
- ➢ Fraudsters ask you to use "request money" option through UPI.
- ➢ Instead of paying money to you, they use app and insist to approve the request to pull money from your bank account.

Precaution to be taken:

- ▪ One should be careful while making financial transactions for online products.
- ▪ Always remember, to receive money there is no need to enter your PIN / password anywhere.
- ▪ If UPI or any other app asks you to enter your PIN to complete transaction, it means you will end up sending money instead of receiving it.

FRAUDS DUE TO UNVERIFIED MALLICIOUS MOBILE APPS

Modus Operandi:

- ➢ Once you download unverified or Malicious Mobile Apps, Fraudsters gain access to your device / Laptop / Desktop.
- ➢ Links for such applications are shared through E-mail/ SMS / social media etc. The links are masked in such a way that it seems authentic but it is redirected to download malicious application.
- ➢ Once the malicious application is downloaded, the fraudster can gain access to the device.

Precaution to be taken:

- ➢ Never download application from unverified / unknown sources.
- ➢ Always download from Google Play Store or App Store only.

ATM CARD SKIMMING

Modus Operandi:

- Fraudsters install skimming devices in ATM machines &steal data from your card.
- PIN is also captured by dummy keypads.
- Fraudsters use the data to create duplicate cards and withdraw amount from customer's account.

Precautions to be taken:

- While making transaction always ensure that there is no extra device attached near card insertion slot.
- Cover the keypad with your hand while entering your PIN.
- Never enter the PIN in the presence of any other person standing close to you.

SIM SWAP/CLONING

Modus Operandi:

- Fraudsters try to gain access to the SIM card or obtain duplicate SIM card for carrying out digital transactions using OTP received on such duplicate SIM.
- Fraudsters posing as Mobile Network Service provider request details for providing additional benefit on SIM Card

Precautions to be taken:

- Never share credentials related to SIM card.
- Be cautious if you are not getting mobile network in your phone for considerable time. Contact mobile operator immediately to ensure that no duplicate SIM is being issued for your SIM.

FRAUDS THROUGH QR SCAN

Modus Operandi:

- Fraudsters often contact customers and trick them into scanning QR codes using payment apps. Fraudsters can withdraw money from customer's account.

Precaution to be taken:

- Be cautious while scanning any QR codes using payment apps.

FRAUDS THROUGH SOCIAL MEDIA

Modus Operandi:

- Fraudsters create fake account on popular social media platforms like Facebook and Instagram.
- Once fake account is created, they send a request to your friends asking for money payments, etc.
- Fraudsters also gain trust over a period of time and can use your Personal information for blackmailing/bullying.

Precautions to be taken:

- Do not make online payments to unknown persons.
- Never share personal and confidential information on social media platforms.
- Always verify authenticity of fund request with the friend by cross checking the same through a phone call to make sure that profile is not impersonated.

JUICE JACKING

Modus Operandi:

- Mobile charging Port can be used for Transfer of Files.
- Juice jacking is a type of cyber fraud, where, once your mobile is connected to unknown / unverified charging ports, malicious software are installed and fraudsters can access your sensitive data and misuse it.

Precautions to be taken:

- Always avoid using public / unknown charging ports / cables.

LOTTERY FRAUD

Modus Operandi:

- Fraudsters send email or make phone call informing you that you have won a huge lottery.
- To receive the amount, it is required to confirm identity by verifying through bank account / credit card on their website from which data is captured by fraudsters.
- Since the requested money is very small percentage of the lottery / prize, the victim falls into the trap of the fraudster and make payment.

Precautions to be taken:

- Never make payments or share secure credentials for lottery calls / emails.
- Always be suspicious when you come across such unbelievable lottery or offers.

ONLINE JOB FRAUD

Modus Operandi:

- Fraudsters create Fake Job portals and lure victims to enter their sensitive information for registration. On entering the details, the account is compromised.
- Fraudsters also pose themselves as officials of a reputed company and confirm selection after doing fake interviews and request money in lieu of it.

Precautions to be taken:

- Genuine company offering job will never ask for money.
- Never make payments on unknown job portals.

OTP BASED FRAUDS

Modus Operandi:

- Fraudsters sent SMS/Emails for offering loans/increase in credit limit and request victims to contact on fraudster's mobile number.
- On calling the Fraudster, victim is asked to fill online form containing financial sensitive information and then convince them to share the OTP or PIN details, resulting in loss of money.

Precautions to be taken:

- Never share OTP/PIN Numbers/Personal Sensitive information in any form to anyone.
- Always keep a tab on SMS/Emails to ensure that no OTP is generated without your knowledge.

LOAN WEBSITES/APP FRAUDS

Modus Operandi:

- There are several Fake Loan Apps/Websites which offer instant Loans.
- These Websites/Apps dupe the borrowers by charging significantly higher interest rates.
- Fraudsters attract borrowers by advertising it as "Limited Period Offer" and ask applicants to make urgent decisions thereby disclosing sensitive information.

Precautions to be taken:

- Always check the genuineness of lender's address & contact information otherwise it may be difficult to contact them later.
- Bank will never ask for payment before processing the loan application.
- Genuine loan providers never provide loans without verifying documents.
- Always download from Google Play Store or App Store only.

BE SAFE & KEEP BANKING