Nation-wide Intensive Awareness Programme 2022 by Reserve Bank of India in collaboration with Regulated Entities

Do's and don'ts for Safe Banking Practices

Do's

- Always go to official websites of banks/service provider and use websites which are secured for e.g. https:// - where 's' stands for secured website.
- Log out of all payment/financial apps from your mobile/laptop/PC if they are facing technical glitches or while downloading apps.
- Check the spellings of websites/URLs being accessed to avoid fraudulent, fake and look-alike websites similar to banks or e-commerce platforms.
- Check spellings and headers of emails received to ensure that the emails are from authentic addresses.
- Be careful while clicking on shortened URLs / google forms received through SMS/ Whatsapp/ email, etc.
- Block/Unsubscribe/ report as spam mails providing links to banks/ecommerce/search engine websites.
- Be careful while buying/selling products online. To receive money through UPI there is no need to enter PIN/password.
- Contact your mobile operator immediately if there is no mobile network in your phone for considerable period of time in a regular environment.
- Check SMS/emails regularly to ensure that no OTP is generated without your prior knowledge.
- Before transacting with any company, verify if they are registered and licensed entity.
- Turn on two factor authentication wherever such facility is available.
- While using ATM, cover key pad with your other hand while entering PIN.
- If cash is not dispensed, press 'Cancel' on ATM and leave only after the home screen appears.
- Note that customer care numbers are never in the form of mobile numbers.
- While depositing cash in CDM, ensure that the cash is accepted by the machine before leaving the premises.
- Always check whether any extra device is attached near card insertion slot or keypad of ATM machine.

Don'ts

- Don't trust strangers and take help from them at ATMs as the credentials may get stolen.
- Don't fall prey to apparently attractive and unrealistic offers.
- Don't share details of SIM card and mobile number or write PIN on ATM card or save details on websites/devices/public laptops/desktops.
- Don't get trapped by offers from persons posing as call centre agents from banks, insurance, government etc. and don't get pressurised/tricked into sharing username, password, card details/PIN/CVV/OTP, date of birth,
- Aadhaar number, names of family members, etc.
- Don't search for contact details of service providers from search engines, SMS, social media, emails, etc.
- Don't click on unknown/unverified links and Don't download apps from unverified sources on advice of unknown people.
- Don't permit your bank accounts/ATM cards to be used by others, for a commission or otherwise, which may lead to police investigation due to misuse of bank account for routing money.
- Don't respond to calls/emails/SMS seeking your KYC details/account details/ATM card details/PIN/CVV/ OTP details.
- Don't trust unbelievable lottery offers and share secure credentials in response to such emails/calls.
- Don't respond to messages claiming that huge amount is lying with RBI and some amount needs to be transferred to get it released.
- Don't get defrauded by paying upfront loan processing fee in cash.
- Don't respond to messages offering/promising prize money, government aid and KYC updation to receive money/recharge mobile balance/to get a job.
- Don't make payments or enter secure credentials against online offers of loans at low interest rate/ secure instant loan.
- Don't use screen sharing apps on the same device where financial apps are being used.
- Don't scan QR codes using unknown payment apps which may be used for transferring money out after keying in the UPI PIN.
- Don't use public charging points or unsecured WiFi as they can be used to transfer malware and take control of data from the phone.

Digital Frauds – Immediate steps to be taken after a fraud

- Contact your bank/NBFC and block your account/card immediately and submit a written complaint.
- Lodge a complaint/FIR with Indian Cyber Crime Coordination Centre or call cybercrime helpline number 1930.
- Contact your branch for blocking funds in beneficiary account(s)
- Escalate matter to RBI Ombudsman if the bank/NBFC fails to resolve your complaint.