Government of India

Digital Transactions

The Indian government recently had initiated the demonetisation drive in November 2016. The demonetization drive resulted into pushing the citizens to carry out banking transactions through Internet or plastic cards. Such technologically driven banking transactions also make banking transactions susceptible to financial frauds.

As the banking sector moves deeper into the digital era where banks provide 24x7 technologically advanced products, the consumers need to exercise greater caution to avoid digital and net banking fraud. It is up to individual customers to ensure the safety and security of their payment systems and enjoy the ease and convenience of digital banking.

The normal mode of cashless transactions is through internet banking, cash cards, wallets, debit cards, credit cards etc. While you enjoy such 24x7 newly-acquired convenience, it is essential to take necessary cautions on cyber security at every step. Here are some of the steps you could take to ensure your financial data is safe.

- Create strong password & PIN, change them frequently. A PIN which is easily guessable is capable of depleting your account balance. Avoid using your date of birth, wedding anniversary, date of birth of family members etc as PIN for your debit/credit cards. While setting passwords, long combinations of alphabets, numbers, and alphanumeric and special characters with mixed casing are advisable. Words that can't be found in dictionaries or that are deliberately misspelt can potentially be stronger passwords. You must memorise a strong password which is unique in nature and can't be guessed by anyone.
- Never write your PIN or password on the cards.
- RBI has already mandated about two-step authentication. The card industry has adopted 3-D secure methodology enabling you to register your smart phone for authentication. It is essential to receive OTP (one time password) which needs to be keyed in at the time of transactions. Delete the OTP which has been received on your registered phone.
- If you receive any such texts or notifications without your trying to log in, you must immediately notify the bank.
- Never respond to the calls seeking details about card numbers, account numbers. Sometime the fraudsters are advising the account holders to switch off the mobiles for sometime on the pretext of updations advising the recipient to switch on the mobile after certain time and seek the OTP to complete the updation process. Please be informed there is no such legal process and hence avoid acting on such advise. If possible inform to the police as a responsible consumer. Incidents have also been reported when such fraudsters also attempt to dupe of your family on the pretext of some mishappening with you.
- **Careful where you swipe at ATMs/ POS terminals.** Scammers can steal your card data through skimmers on bugged ATMs and point-of-sale machines. Make sure you use your cards at secure ATMs and shopping outlets only. Using chip-less card always put you at a higher risk. Indian banks have already been mandated to upgrade all cards to chipped cards.
- When making a purchase, ensure that the salesperson processes your transaction in your presence. Check your card when it is returned to you by the cashier to ensure that it is yours and that it has not been tampered with any way. Total your charge slip before signing in, as blank spaces serve as an invitation for unscrupulous individuals to ass additional amounts.

STATE CONSUMER HELPLINE
KNOWLEDGE RESOURCE MANAGEMENT PORTAL
Centre for Consumer Studies, Indian Institute of Public Administration, New Delhi
Phone - (011) 23705055 , TELEFAX - (011) 23705054
Email - schkrmp.iipa@gmail.com
Website - www.consumeradvice.in, www.consumereducation.in

- Do not withdraw the money from the ATMs if you find anyone standing inside the ATM. Many a times, it has been reported that the cards have been exchanged intentionally by the persons standing in the ATM area assisting the account holders for transactions.
- Avoid sharing any sensitive information to the callers seeking details on the pretext of expiry of cards, blocking of transaction limits etc. No one including the bank officials have been authorised to seek such details.
- Use a power-on/access password for your computer, laptop and mobile as well as a screensaver password so that no one else can access your systems without consent. Change your passwords and security settings regularly.
- Always visit your bank's secure Internet Banking site directly. Avoid accessing the site through a third-party link or via email. Verify the domain name before you try to log in.
- Log out of your Internet Banking account the minute you complete transactions. Do not close the window without logging off.
- Avoid using Internet Banking on unsecured WI-FI networks such as railway stations, airports and cybercafés.
- Install authentic security programmes to guard your system and account against hackers, virus attacks and other malware. Update the security programme or antivirus regularly.
- Install a suitable firewall to protect your computer or laptop and its contents. Never provide remote access to your system to anyone; not even family members, as it is still vulnerable to hacking.
- Disable the 'File and Printing Sharing' command on the operating system.
- Always log off your PC or laptop when not in use; don't keep it lying around or trust a stranger with it.
- Never save your mobile banking log-in and password on the phone. Either memorise it or write it down somewhere else.
- Never leave your handset unattended and logged into a mobile banking app.
- Always lock your phone to prevent unauthorised use.
- Notify your bank as soon as your mobile is lost or stolen.
- Update the mobile banking app as and when a new version/upgrade is released. Also update your phone with latest security patches.
- Never download apps from untrustworthy and dubious sources.
- Always log out of your banking app after using it.
- Keep an eye on your account balance and transaction history regularly.
- If you suspect unauthorised transactions on your account, report it to your bank immediately or at least within three working days, so that your complaint/grievance is addressed in your favour. Any delay can leave you with a liability or financially poorer.
- **Third-party apps and downloads.** There is always a temptation, especially for Android users, to download something from the net instead from the Play Store. While Play Store vets most of the apps that are available on the platform, internet providers have no such obligation. Most of the sites that allow these downloads come with viruses and malware that can easily infiltrate and collect user information from your device. Play Store may not have everything or may have apps that are expensive, but that is the price you pay for security.
- **SIM swap:** The fraudsters will first collect your personal banking information through phishing, vishing, smishing or any other means. Once they have your personal information, they get your SIM blocked, and obtain a duplicate one by visiting the mobile operator's retail outlet with fake identity proof. The mobile operator deactivates the genuine SIM card, which was blocked, and issues a new SIM to the fraudsters.

It is now simple to generate a one-time password (OTP) required for transactions using the stolen banking information. This OTP is received on the new SIM held by the fraudsters and they can now transact before the bank customer realizes the theft and alerts the bank. Please report the matter to the Bank and Police if you find your mobile was deactivated even for sometime.

- If you have been a victim of any of the financial frauds, what should you do? As per RBI directives on “Frauds—classification and reporting”, the Reserve Bank of India has put the responsibility to provide protection against and fight frauds on banks, exposing them to a completely new horizon of financial risks. Further, banks are now required to report to the RBI complete information on frauds and the follow-up action. The RBI has also issued operative guidelines to regulate this channel, suggesting reporting of suspicious transactions to its financial intelligence unit. “To keep a check on frauds, banks need to incorporate a greater level of scrutiny by deploying advanced tools and technology capable of protecting the customers against unethical activities,”
- While banks are mandated to prevent frauds, you, too, can take some steps to protect yourself. Ethical hackers—people who hack to evaluate level of security and without any malicious intent—say that users should be especially careful when using banking or other apps on which financial transactions can be conducted.
- Don’t jailbreak your phone. Jailbreaking is the process of removing hardware restrictions and thus allowing free apps.
- Check what you download and run on your phone. “For example, don’t use WhatsApp for confidential communication; use an encrypted app instead,” .
- You may want to limit debit card usage at PoS machines and use it only as an ATM card for cash withdrawal. “Try to use credit cards at PoS because if a fraud takes place, you can raise a dispute, and it is not your money,”. Be cautious at ATMs; look around for suspicious objects or hidden cameras above the keyboard.
- You may rub off the CVV number as written on the reverse of the card. Memorize the CVV number before rubbing, so that you can continue using the card. Use computers that have anti-virus software. Don’t share passwords, PINs and OTPs with anyone regardless of the reason stated. Banks never call asking for OTP details. Do not log into links sent on emails that require you to revalidate your credentials on account of a system upgrade. For apps, download directly from an app store; don’t click on unknown links or those sent by unknown numbers.
- Complaints: Many a times following complaints are reported.
- Transaction succeeded with deduction of the amount from the bank account but the credit could not be afforded to the Merchant.
- Fraudulent transactions.
- In case you are transferring the amount to another account, please ensure that the details of the beneficiary like name, account number and bank name are correct. In case of any wrong transfer, it would not be possible to reverse the transaction. You might have to request the wrong beneficiary to seek and refund/return.
- Avoid transactions at cyber cafes as the cyber cafe may be adapting to some illegal software's to save the details of user ids and password.
- In case you are initiating payment of utility bills like telephone/ mobile bills, electricity bills etc. please ensure that the bill details are entered correct else the payment made to wrong bills can never be refunded or reversed.
- Register your mobile number and email id with the bank/ card issuer for any transaction alerts.

- Many merchants, banks are charging transaction fee for making payments through debit/ credit/ cash cards, internet banking etc. Please study such terms before initiating any such payment.

- General Transaction Failures.

following could happen:

1. Payment deducted from the account but there is a failure at payment gateway due to bad connectivity, server problem etc.
2. The payment succeeded at payment gateway but failed while being transferred from the payment gateway to the merchant/beneficiary.

- Payment gateways companies are required to settle payments with banks every day and hence any payment not reaching the payment gateway due to bad connectivity, server problem should get back to the account holder within two working days.
- In case the payment could not reach the merchant or beneficiary account, the payment should get transferred to the merchant//beneficiary within two working days. The consumers may take up the complaints of unsuccessful transactions keeping all the three institutions like Bank, Payment Gateway and the Beneficiary or Merchant in loop.
- The unsuccessful transaction of withdrawal of cash from ATM cards using debit cards should get resolved within 7 days of making complaint to the bank with which the consumer has account irrespective of whichever the bank the card is being used for cash withdrawal. Any delay beyond 7 working days of the complaints, the bank is required to pay penalty @ Rs. 100/- per day of default.
- In case of payment failure while making payment through the wallets, the debited amount should get credited back immediately.

STATE CONSUMER HELPLINES

Andhra Pradesh	1800-425-0082,1800-425-2977	Odisha	1800-345-6724,1800-3456760
Bihar	1800-345-6188	Puducherry	1800-425-1082,1800-425-1083,1800-425-1084,1800-425-1085
Gujarat	1800-233-0222,079-27489945,079-27489946	Rajasthan	1800-180-6030
Haryana	1800-180-2087	Tamilnadu	044-28592828
Himachal Pradesh	1800-180-8026	Telangana	1800-425-00333
Jharkhand	1800-3456-598	Tripura	1800-345-3665
Madhya Pradesh	155343,0755-2559778,0755-2559993	Uttar Pradesh	1800-1800-300
Maharashtra	1800-22-2262	Uttrakhand	1800-180-4188
Mizoram	1800-345-3891	West Bengal	1800-345-2808