Judicial Academy Jharkhand

झारखण्ड राज्य विधिक सेवा प्राधिकार
न्याय सब के लिए
JHARKHAND STATE LEGAL SERVICES AUTHORITY
ACCESS TO JUSTICE FOR ALL

General Instructions To PREVENT CYBER CRIME

(For Common Man)

General Instructions To Prevent Cyber Crime
(For Common Man)

Due Diligence for Preventing Cyber Crimes - India is the third largest user of Internet in the world today. We use mobile phones and computers for carrying out banking transactions, shopping and other day to day activities. Internet, mobile phones and computers are used in abundance leading to increase in cases of Cyber Crime, however a digitally literate and well informed citizen can avoid a number of Cyber Crimes from taking place.

1. SECURITY PROTOCOL FOR THE USE OF INTERNET

Standard Precautions :

Dont's

- Do not download files from unknown sources.
- Do not download drivers etc. from popup Windows.
- Do not install software from unknown sources on your computers devices.
- Do not click on any unknown link sent through Facebook or WhatsApp or any other mode of communication or messaging platforms.
- Do not browse for customer care number of any company on Google. Visit the official website of the company or call on the toll free number listed on official websites.
- Do not display your private data like date of birth/bank registered phone number etc. on social media profiles as they might be used for data mining and hacking through social engineering.
- Do not submit personal /financial information on Google forms created and sent by unknown sources or shared through WhatsApp/SMSs. Bank or any other financial institution do not ask such information through such medium

Do's

- Personal details like PIN, CVV number, passwords etc. must be kept safe and one should not share Debit Card/Credit Card Number, PIN, CVV number etc.
- Install a strong firewall/antivirus to prevent unauthorised access.
- Proxy servers and routers should be configured with adequate security.
- View the security status before entering private/personal information like username and password on any website.

- Use E-commerce services of secure sites. Exercise caution in downloading E-commerce application from Google Play Store.

2. SAFE e-MAIL SYSTEM

Standard Precautions :

Don'ts

- Do not reply to unknown emails and one should not open the attachments with such unknown emails.
- Do not click on unknown links sent through emails disguised as jokes, videos etc.
- Do not share PIN, OTP, passwords etc. with anybody.

Do's

- Use a strong password.
- The best passwords are normally made by using special characters and alphanumeric passwords with both uppercase and lowercase characters. Like (Abc#12*@$)
- 8 to 10 digits password is considered to be strong.
- One must not share vital information over shared computers/ cyber cafe and preferably one must use a personal computer or device for banking transactions etc. or should use virtual keyboards.
- Screen lock and app lock options should be used.
- One must logout from the website after use.
- Sensitive information must be saved in encrypted form in a file or hard disc or at least it should be password protected.
- As a safety measure computer system should be enabled with security enabled login and after finishing the work or at the end of the day the computer must be switched off and internet should be disconnected.

3. SAFE USE OF ATM

Standard Precautions :

Don'ts

- Do not keep the ATM card and PIN (written on a piece of paper) together in a purse or wallet.
- Do not share the 16 digit of the credit/debit card along with PIN or CVV. Bank officials never ask for the same over telephone or email for any purpose.

- Do not write the PIN on the front or on the reverse side of the card or on the cover of the ATM card.
- Do not enter the PIN or CVV in such a manner that anybody is able to read it.
- Do not use date of birth, phone number etc. as pin or password, as it can be easily guessed.
- Any email or message received regarding ATM PIN should never be replied these are phishing attacks.

- One should never share information relating to ATM card, PIN, OTP, CVV etc. over telephone or email.
- One should not take help of any stranger or even the guard at the ATM machines for use of ATM cards.
- While using ATM card one should not indulge in unnecessary talk with strangers

Do's

- The ATMs where security guards are deployed by the bank are normally the safest to use. One should frequent to a safe ATM machine.
- Keep the card in safe custody and it should not be handed over to anybody for any purpose.
- Remember the PIN and all other physical records of PIN must be destroyed.
- One must keep a strong PIN of the Debit/Credit cards.
- Request the bank to enable SMS services relating to banking transactions and the mobile number must be updated regularly in bank records. The SMS-alert services should always be kept active to be informed about any fraudulent transaction and also for the purpose that the information regarding banking transactions are received in time.
- In case there is any unauthorised transactions relating to ATM card the bank must be informed immediately to prevent misuse of ATM card.
- While using ATM card one should be vigilant about any suspicious activities in vicinity.
- Check for presence of any external accessories like skimmers/spy cameras in the ATM machines.
- Please check external accessories like skimmer, labenese loop,spy cameras before using ATM machine.
- While transacting at ATM if any suspicious thing is detected, the transaction must be cancelled by pressing the "CANCEL" button on the ATM.

- Enter the PIN in an ATM machine or POS machine by covering the keypad with the other hand so that any fraudster may not be able to read the finger movement.
- Collect the cash and ATM card from the ATM machine before leaving it.

4. IN CASES WHERE THE PAYMENT IS DONE BY SWIPING CARD AT PoS MACHINES:

Standard Precautions :

Don'ts

- Never share the PIN with the merchant.
- Never handover the ATM Card to the merchant.
- Don't get distracted till transection gets complete.

Do's

- Verify the amount entered in the PoS machine before making payment.
- While swiping card at any PoS machine the card must not be handed over to anybody as transaction can be made by bypassing PIN or the Card number may be recorded and other unauthorised transaction may be carried out using the same details later.
- In case of loss of ATM card it must be blocked by informing the concerned bank on the toll free number printed on the reverse side of the ATM Card or through email. The concerned bank branch must also be intimated immediately.
- In case of cards whose validity has expired, they must be destroyed in such a manner that the magnetic strip is also get destroyed, as the magnetic strip contains readable details of the customer which can be misused.
- In case you find any device or suspicious thing connected/superimposed on any ATM machine one must avoid carrying out transaction and the matter should be informed to the concerned bank immediately.

5. e-COMMERCE :

e-commerce is the activity for sale and purchase of commodities and services etc. using internet in most of the times. The online mode of payment like ATM, online banking and pay wallets are used for making payment while carrying out payment on e-Commerce sites. Most common e-Commerce sites are IRCTC for booking tickets, Flipkart, Amazon, Myntra, Snapdeal and Ebay for online shopping and Paytm, BHIM app etc. for mobile recharge, electricity bill payments, etc.

Standard Precautions :

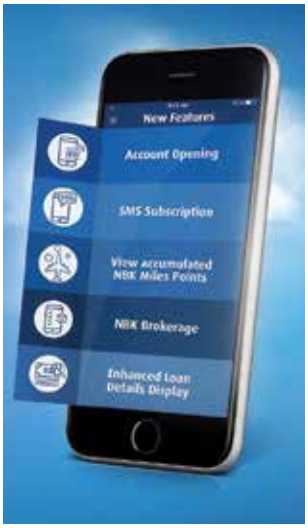
Don'ts

- Do not share card number as well as CVV mentioned on the back of the card with anybody.
- Do not respond to telephone calls and email messages giving lucrative offers and one must not share banking details like OTP or any link received via email or SMS with such persons. Personal details should also never be shared with them.
- Do not use websites without verifying the credentials regarding their postal address etc.

Do's

- If there is any doubt about email received, the details of the sender must be verified. In case of receipt of any request for transfer of money by sending any distress message it must be verified first and then only the money be transferred.
- An e-wallet or cards should be used for payments but it should be used only on secured sites. A secured site is one which starts with "https://....." and not with "http://.....".
- Websites of e-commerce websites must be visited only after viewing their security status :
- To check a site's security, to the left of the web address, look at the security status:
  - Secure
  - Info or Not secure
  - Not secure or Dangerous
- One must check his bank account and statement of account regularly and one should not share bank account number, card number, PIN, OTP, UID etc. with anybody under any circumstances.
- The PIN number should be changed frequently and one should not use the common passwords for a number of accounts.
- Genuine and good "antivirus" and "anti-Malware" software must be installed on the computer or mobile devices.
- One must read carefully the details given on the online shopping portals and may preserve printouts prior to shopping on online portals and sites.
- One must read the return policy, order cancellation policy, option to pay cash on delivery and address to which the goods are to be returned etc. carefully.

6. MOBILE BANKING SAFETY PROTOCOL :



After the inception of the Digital India plan, there is a huge leap seen among common man from cash to cashless transactions as envisaged for the cashless economy. Unified Payment Interface (UPI), Digital Wallets, cardless transactions, m-banking are the emerging mode of banking transactions.

Standard Precautions :

Don'ts

- Do not keep the phone/device setting permitting the phone/ device to remember user ID, banking details, passwords and other personal information. As in case the mobile device goes to a wrong hand it will go with all the details including passwords.
- The transactions must be protected with dual security which means every transaction must be authorised by OTP.
- One must frequently check emails and SMS relating to banking transactions.
- In case one is having trouble in using internet connection through his own mobile phone data pack, one should avoid doing banking transactions on shared Wi-Fi or hotspot. There are chances of data theft while using free Wi-Fi or Hotspots.
- One should never share any link received by messaging or email
- One should also not share personal information like bank account numbers or PIN, CVV and OTP with anybody.
- One must not respond to phone calls purported to be made from bank or banking officials and even if you receive it no personal details should be shared over phone. Banks never ask for personal information like OTP etc. over telephone.

Do's

- Disallow cookies in the internet setting on the device where internet banking is frequently used.
- Two step verification must be set up to login into the m-banking profile.
- While downloading and activating mobile banking apps one must carefully check the description of the site and the source from which it is downloaded. Only authentic apps from authorised banking sites and Google Play Store etc. should be used.
- One must use dual security for banking transaction that is, apart from login every transaction must be authenticated by OTP.
- One must use screen lock as well as app lock for banking apps.
- One must keep the phone software updated and antivirus software must also be used to keep the phone safe.
- After completion of banking transaction one must log out from the app.

Note :-

- In case anyone becomes a victim of Cyber Crime, an FIR should be lodged at the nearest police station.
- One may also file a complaint in the nearest Court of law with a prayer to transfer it to the the police station of competent jurisdiction.
- Application can also be filed under the provisions of section 43 A of the IT Act for grant of compensation before the competent authority which as per the notification of Ministry of Information Technology is the Secretary of the Department Of Information Technology in all the states.
- RBI has also issued circular bearing number RBI/ 2017-18 /15 DBR. No. Leg. BC. 78 /09.07.005 / 2017-18 dated July 6, 2017 which provides Customer Protection in cases of Unauthorised Electronic Banking Transactions.
- Banks must provide customers with 24x7 access through multiple channels (via website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorised transactions that have taken place and/ or loss or theft of payment instrument such as card, etc.
- According to Master Circular of RBI, bearing number RBI/ 2017-18 /15 DBR. No. Leg. BC. 78 /09.07.005/ 2017-18 dated July 6, 2017, in cases of Limited Liability of a Customer and Zero Liability of a Customer- A customer shall not be liable for loss in the following events:

  (i) Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).

  (ii) Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorised transaction, that is in case the banking details have not been shared by the user the concerned Bank will indemnify the amount lost through online transaction.

❑❑❑

JUDICIAL ACADEMY JHARKHAND
Near Dhurwa Dam, Dhurwa, Ranchi-834004
Phone : 0651-2902833, 2902831, Fax : 0651-2902834, 2902831
Email : judicialacademyjharkhand@yahoo.co.in
Website : www.jajharkhand.in

JHARKHAND STATE LEGAL SERVICES AUTHORITY
NYAYA SADAN, Near A.G. Office, Doranda, Ranchi
Phone : 0651-2481520, Fax : 0651-2482397
Email : jhalsaranchi@gmail.com
Website : www.jhalsa.org