HOW TO AVOID DEBIT OR ATM CARD/CREDIT CARD FRAUD

SOCIAL ENGINEERING ALERT: - Never disclose your card details and other security details such as PIN, CVV or OTP to any one over phone or email, who claims to be bank personnel or from any other agency, informing you regarding card being blocked and their offer to assist in unblocking the card. If you feel that your card is blocked or not functioning contact your bank in person.

TIMELY DELIVERY OF CARD AND PIN: - Ensure that you receive your requested card and Pin within the reasonable time, if not contact the bank immediately to rule out the card and Pin landing in the hands of some other person.

CARD PROTECTION: - Store your card at a safe place.

CONFIDENTIALITY:- Keep your Card details, PIN number and CVV secret, discard the practice of writing your PIN number on the back of the card or at a place where it can be easily noticed by someone. Memories the CVV (Card Verification Value) number and erase it from the back of Credit card.

SELF USEAGE: - Always try to use the card from your hand or through a reliable person. Never request others such at ATM security guard, or other ATM users to operate your card.

SAFE TERMINAL: - Ensure that while using your card at an ATM or POS, no any external/ additional devices are attached to the card slot.

AVOID SHOULDER SURFING: - While typing/entering your PIN number at an ATM or POS, make sure that the keypad is sufficiently obscured from being viewed by an onlooker.

AVOID SCHEMING/CLONING: - Ensure that the card is swiped in your presence. Do not allow your card to be taken for any transaction beyond your visibility.

USE SECURE SITES: - Ensure that when you are on merchant sites or on payment gateways, the site is exactly the same which you intend to visit and is SSL certified, meaning the sites web address starts with https, (the word 'S') and it's in Green colour with a PadLock symbol.

DUMPSTERS DRIVE: - Transaction slips generated which are no more required should be properly disposed off.

PERIOD CHECK OF TRANSCTION:- Regularly check your transaction details and ensure that each of the transaction was done by you, if not imminently contact your bank and the Cyber Crime Cell.

For any assistance please contact Cyber Crime PS,
Phone 0832-2443201
Email: - picyber@goapolice.gov.in