CRIME PREVENTION - TIPS

Certain simple precautions taken up by the public can go a long way in making policing more effective and reducing crime opportunities. Some of these precautions, which can be adopted by the public, are listed below. This is not an exhaustive list but an indicative one.

Fictitious offer of Funds

- Fictitious offer of funds to general public through letters, e-mails, mobile phones, SMSs etc. To lend credence to such offers, the communication is often sent on/from letterheads/websites that purportedly signed by top executives/senior officials of such authorities. While names of the officials might be correct but their signatures are fake.
- The fraudsters initially ask potential victims to deposit small sums of money for reasons, such as, processing fees/transaction fees/tax clearance charges/ conversion charges, clearing fees, etc. The victims are asked to deposit the money in a specified account in a bank. The fraudsters often have multiple accounts in the names of individuals or proprietary concerns in different bank branches for collecting such charges. Genuine but gullible account holders are persuaded by the fraudsters to even lend their accounts for such fraudulent activities on the promise of receiving some commission.
- The general public can report such incidents immediately to the police /Cyber Cell /Economic offences Wing or use **online information** form to inform any such incidents.

Doors And Windows

- Always keep your main door closed even in daytime. Provide it with a peephole.
- Fix a metal grill or collapsible gate outside the main door, which will provide you the visibility without exposing you to threats.
- Install magic eye and safety chains on doors. Look through the magic eye and ensure the door chain is secure, before opening the door to a stranger.
- Ensure that the window grills are not screwed into the frames, but embedded in the cement work.
- Whenever you move into a new house, change the main door and back door locks.
- Where air-conditioners are fixed provide an additional grill outside.
- There is generally a spate of 'window snatching' during the hot summer months. The public is advised to sleep at a certain distance from the open windows.
- Do not keep valuables, purses, mobile phones, and wristwatches openly visible from outside. If possible fix mosquito nets on the nets, which won't cut off ventilation.
- Fix Electronic burglar alarms with telephone for warning.

- Inform your neighbors about your absence from your home for a long or short period.
- Don't keep the keys of the receptacles in which the valuables are kept in the convenient places like under the door mat or in flower pot, etc., not allowing access to strangers.
- Don't allow any stranger to enter your house, when you are alone without finding out his identity. Always ask representatives to provide identification.
- Beware of persons coming to your house under the pretext of repairing/selling things, conducting meter readings etc.
- Do not record a message on answering machine telling people you are on holiday or away.
- Always identify a visitor before opening the door. Never allow young children to open the door to visitors.
- Don't keep huge amount of cash and ornaments in the house, Use Bank lockers.
- Don't disturb the scene, if you notice theft in your house, wait for the arrival of police otherwise it will lead to tampering of evidence like fingerprints, footprints etc.

Lighting

- Switch on outside lights during nighttime.
- When you go out, switch on at least one inside light, to give the impression that the house is not empty.
- There are timer mechanisms available in the market, which control lights. If you are planning to be away from home for some days, install one of these gadgets. [TOP]

Attention Diversion :

Vivek withdrew Rs.5,00,000/- from Bank and kept the cash bag with him in his car. While he was proceeding towards Mount road, at traffic signal one stranger told him to check his deflated rear tyre. On this, he came out from the car leaving the cash bag in car, and checked the air and found that everything is alright. But in the mean time, another person has taken the cash bag from the car and fled away (True Story)

- Divert the attention by throwing small currency on the floor and ask you whether those notes belong to you. Don’t divert your attention for the small currency especially when you are in bank and making huge transactions.
- Some will approach you with a story that their relatives are in hospital and they are likely to get money from their village and ask for your account details to credit their money.
- Some follow you till your home and when you stop midway to have tea or shopping, open your dickey

to steal your money.

- Don’t alight from your vehicle immediately after you are told about the problem in the tyres of car.
- Whenever you withdraw huge amount from bank better take somebody with you.

HOME DIVERSION BURGLARY

- One individual will approach the victim and occupy his/her attention while a second subject enters the victim's home and steals cash, jewelry and silver.
- Another home diversion techniques is for perpetrators to come to a residence and ask for a drink of water, use a bathroom, or use a telephone for an emergency to gain entrance to a home. The subjects will then attempt to divert the victim's attention while an accomplice searches for valuables.

  Tips: If an unknown subject comes to your home seeking directions, the phone, the bathroom, etc., keep the subjects outside the home and at least one locked door between you and them. If they need water direct them to an outside faucet, if they need to contact someone, offer to make the call for them.

Phishing

Santosh (victim) got an email from alleged ICICI Bank that his account needs update. When victim clicked on the link provided in the email (one must never do this…!) it re-directs to fake ICICI bank Page. As the Page is a look alike of ICICI bank Page, the unassuming victim entered his username and password of the bank account along with his details asked there. Within a span of ten minutes, Rs.5,05,000 were withdrawn from his account by some unknown persons in six transactions and the amounts were transferred to various accounts in ICICI bank accounts across India.

What is Phishing?

- Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by posing as a trustworthy site in an electronic communication. Most of the online banks are common targets. Phishing is typically carried out by e-mail or instant messaging, and often directs users to enter details at a website, although phone contact has also been used at times.

How to Spot Phishing Emails

The best way to avoid becoming a phishing scam victim is to use your best judgment. No financial institution with any sense will email you and ask you to input all of your sensitive information. In fact, most institutions are informing customers that "We will never ask you for your personal information via phone or email".

Safety tips to avoid Phishing?

When you receive emails claiming to be sent by banking institution asking you to enter your account details, DO NOT do so! Your bank already has your details and clearly would not want them again.

- Check if the email that you receive has your name spelt correctly. Fraudsters simply try to guess your name by your email address. DO NOT open emails that have your name spelt incorrectly.
- DO NOT respond to emails that seem like they are sent from your bank. Some of the claims made in these emails may be the following:

  -You are to receive a refund
  - The bank is trying to protect you from a fraud
  - The bank needs some security and maintenance update on your account
- If you receive such email always check back with your bank directly or speak to the customer service representative of the bank.
- NEVER enter your credit card details and password in a website which you suspect is not genuine.
- It is a good practice to type in the URL of your bank yourself, or bookmark it if the URL is difficult to remember.
- DO NOT follow links to a banking website from another website or email.
- Verify a website's URL carefully before you provide your login details on any web page. Fraudsters create fake websites that have URLs closely resembling the original.
- DO NOT share your account details, password, or credit card details with anyone who you do not know or trust.
- Log in to your accounts regularly and look for account transactions that you do not recognize.
- DO NOT send your account details and/or password over an email to anyone.

Password:

Important tips to keep your password safe in the Cyber World.

- Never tell or share your password or with anyone.
- Never write your password on the paper, or send your password in Email or tell your password over telephone.
- Always change your password regularly.
- Avoid choosing the "Remember/Save my password" option.
- Avoid typing the password in-front of others.
- Always use the different passwords for different logins.

Do's

- Use a password with mixed-case letters (eg, AaBb) and use upper-case letters in the middle and/or end, not just the beginning.
- Use a password that is easy to remember, so you don't have to write it down.
- Use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder
- Passwords are the secret which is used to protect the valuable personal information that is stored in our computer and in our Online Accounts.

Don'ts

- Don't tell a password over the phone to ANYONE.
- Don't reveal a password in a email message.
- Don't talk about a password in front of others.
- Don't use the "Remember Password" feature of applications (For Example, OutLook, Browser, Messenger)
- Don't share a password with family members.

Matrimonial sites

Now a days to have easier methods of getting married, young generation register themselves on various matrimonial sites. These sites enable to find match to the needy people. It also saves the time from going one place to another. But before registering onto these matrimonial sites always check credentials of the site.

- For choosing partner from the matrimonial site first it is important to find out that whether that site is registered or not.
- How many people are aware of that site? That can be done through by asking people or friends.

- To find out the qualification it is important to check the certificates. Sometimes wrong qualification or job description is given. It is done to attract the looker.
- For job description find out the place and period of working. It can be done by giving call or visiting the office by surprise. If it is nearby then spend some time to find out that whether that person is working or not.
- **If the person is NRI:** In such cases it is difficult to find out the actual person. For that proper research should be done. If it is inter religion, find out the type of culture and living standard. Friends and relatives can be good option for enquiring

What is 419 Advance Fee Fraud?

Mr. Sankar is a retired executive from a public sector undertaking received a mail from an unknown person, Mr. Michael asking for my assistance in retrieving five hundred million looted U.S. dollars for a twenty-five percent reward. Excitement raced through him. Sankar requested for more information. Second e-mail provided him a phone number. An 'attorney' in the UK told him that he would receive twenty installments of twenty-five million dollars, deposited into my bank account biweekly. All he needed to do was pay twenty-five thousand dollars in expenses and up-front fees (advance fee).

Sankar patiently waits for the booty, it doesn't come. He calls up the the UK number desperately only to hear Michael saying money is stuck in Delhi Airport and he needs more money to get it released. Unsuspecting Sankar sends some more money to the account number provided by Michael. Sankar continues to wait for his booty even today…..! Sankar is scammed.

Warning signs of a 419 Nigerian Advanced Fee Fraud Scam email

- A promise to share or transfer millions of dollars to you for your help or participation.**(Out of 6 billion people in the world you were singled out as this fortunate person, lucky you…!).**
- The e-mail or correspondence is marked "**urgent**," "**top secret**" or "**highly confidential**" and demands you act immediately. **(Time is commonly of the essence).**
- The sender claims to be an exiled **Dignitary, Cabinet Member, General, CEO, CFO, lawyer, doctor or the heir** of some other important person or top official to gain your confidence. **(The Grifter usually uses a Hotmail, Yahoo, Netscape or other such free and anonymous e-mail service to send you the message - not very Regal at all).**
- Claims to have obtained your e-mail address "**during a personal research on the Internet**" or from an unidentified "friend who was once on diplomatic mission.
- The proposal contains a seemingly unlikely situation, i.e. overpaid millions on a contract, royal money or assets frozen by a foreign government, an inheritance, or money, gold or diamonds that need to immediately be transferred or be lost forever.

- Seeks an "**honest foreign partner**" to help with them with their crisis situation. **(As if none exist or can be found in their own country).**
- States they are working with an unidentfied "**Security Company**" or the "**Central Bank of Nigeria**"
- Requests personal information from you, i.e. your full name, bank account information and routing numbers, home or business telephone and facsimile numbers, or a copy of your letterhead.

Tips to Avoid 419 Advance Fee Fraud

- The best tip is to **DELETE** any mail from a stranger which resembles the mails we described above
- Same mail may be forwarded to the service provider's mail ID like **abuse@yahoo.com, abuse@hotmail.com** depending on the senders mail ID.
- Similarly you can forward the mail before you junk it to local police email ID if they have any

Credit Card Users

- In case of losing the credit card, lodge a complaint with the bank immediately. It will enable the bank to announce it as 'hot card' as early as possible, making it possible to nab the culprit. This will also protect you from liabilities, which may be incurred using the stolen card.
- Do not write the PIN number on the card itself.
- Always check your monthly bank statements for any suspicious transactions
- A card's magnetic strip has the basic details of the cardholder. But the card also comes with a blank space for you to sign in. You must sign on the card to avoid unauthorized use.
- Better hang around when your card is being swiped.
- Disable your credit card account if you are not using it.
- Do not store your personal and credit card information on the computer
- Never delay to report a lost credit card as the consequences can be highly disastrous.
- Thoroughly check the authenticity of the firm, the website, or any other transactional society where your money would be flowing through.

Using An ATM

- When you type your PIN number at an ATM, make sure that you sufficiently obscure the keypad from being viewed by an onlooker
- Make sure your privacy is not intruded while using the ATM

- Collect the cash and count it as unobtrusively as possible.
- Keep the cash in its place before coming out of the ATM booth
- Make sure you log out in the right sequence
- Don't forget to collect the card from the slot.
- Do not ask for assistance from any unauthorized person.
- Do not encourage strangers who offer unsolicited advice.
- Avoid using ATMs in uncrowned places especially late night
- When signing the bill counterfoil, after making a purchase using the credit card, make sure there are no duplicates or additional bills.

Parents Guide to INTERNET safety

Parents should recognize the benefits that the internet offers but should also be aware of the potential dangers online. The naive and trusting nature of children can make them an easy target for a variety of dangers on the internet like bullying and harassment, pornography, information theft and financial fraud. However, if parents take the time to educate themselves about technology and establish some simple safety rules, the internet can become a very positive and educative place for their children.

Some warning signs to watch for...

- Changes in your child's behaviour such as being very secretive or sudden changes in their interests, problems with sleeping and so on.
- The amount of time that your child spends on the Internet, especially if this is late at night.
- Your child becoming secretive or defensive about his online activity and quickly changes the screen when you enter the room
- Unusual charges on your phone/internet bills.

Things to do to ensure CYBER SAFETY OF YOUR KIDS:

- Educating your child about the internet is the most effective way of protecting them against the dangers that lurk online.
- Spent time with them to explore the internet and to introduce them to appropriate websites of their interest.
- Set the rules for internet use , limit the number of hours and times at which they can be online

- Install both commercial and free software that create a safety system for your computer.
- Place the computer in a neutral space in the house e.g. the living room.

Do's:

- Encourage your child, to inform you immediately if they are threatened, scared or made uncomfortable by someone or something online.
- Advice your child to be cautious about believing what they read on the Internet, because it is not always true or reliable.
- Alert your child to be careful when they visit chat rooms and keep out of chat rooms for adults under all circumstances.
- Instruct your child to make sure that the firewall software is alway running when they use the Internet connection. Under no circumstances must this be switched off.

Don'ts:

- Instruct your children not to give their own or their friends names, addresses, phone numbers, school names, or other personal information.
- Instruct your children not to send any picture of themselves, their parents or their friends to anyone without your permission.
- Instruct your children not to fill out forms or questionnaires online in your absense or without your permission.
- Instruct your children not to enter areas of website that have charge for services without your permission.

Things to do if your Child is a victim:

E-Mail Offences:

- Take the child in to confidence, get the information of the email ID from which such emails are received, get the prints of the concerned emails along with the full header.
- Save the emails, do not delete it from the inbox. Initially ,there is a tendency to delete immediately when such type of emails are received. Don't do this. Save all the emails beginning from the first one .
- The ISPs normally preserve log details for a very short duration, which may vary from fifteen days to two months, do not delay in approaching the police. It may result in evidence getting lost.

- Submits email prints with 'full header' along with the complaint to the police. Do not reply to unknown email Ids.

Creation of Vulgur /obscene profiles:

- various service providers allow creation of personal profile, but unscrupulous elements can misuse this, when the girl has a difference of opinion or a misunderstanding with a male friend. The male friend or his friends create a vulgar/obscene profile of the girl and post it on such websites along with the phone number.
- The girl may then receive obscene and harassing phone calls from all over the world. In such a case, enquire with the people who are calling to identity the ID of the profile, that it can be removed by requesting the website administrator.
- Take a print of such a profile and submit to the police.

Obscene/Vulgar SMS /MMS Clipping:

- The service providers do not keep record for more than two days, therefore if objectionable MMS clippings are received; contact the police/cyber crime Investigation Cell, immediately.
- Whoever transmits obscene or Vulgar SMS/MMS messages commits an offence, For e.g. If 'A' transmits to 'B' and 'B' to 'C' etc. then "A" & "B' had committed an offence. So do NOT transmit any message that is vulgar.

Security

- Ensure your watchman is an able bodied person. Do approach the local police to verify his antecedents.
- Surprise the watchman at wee hours to ensure he doesn't sleep.
- Organise night patrols in your community. The local police will assist you if approached through the residents' association.
- Keep touch with the beat police constables while they are coming to your area and keep them informed of even minor incidences. This will prevent major crimes in future.
- Don't allow strangers who claim to be mechanics / messengers / sales people to enter, without thoroughly checking their credentials. Train your watchman also to do so.
- Don't hesitate to report crime or suspicious activities, Inform the local police .

- If at all you have to allow them inside when you are alone, call the watchman or a neighbour to stay around till the work is completed
- Inform without delay of any gambling activities, pirated/ porno CD distribution, drug or illicit peddling in your locality. Any hesitation will result in increase of criminal elements in your locality
- Remember. The more you deny temptation, lesser will be the chances of being robbed.

Jewels / Cash / Documents

- Keep jewels, important documents and other valuables in bank lockers. Bring them home only when absolutely necessary.
- Don't keep valuables or money in the side box of your parked two-wheeler.
- Don't leave valuables or money in your Car while parking.
- Ladies are advised to conceal their neck jewels while traveling in public transportations and during public festivals.
- If you are coming out of the bank after heavy withdrawals or out of a jeweler after purchase, be alert of somebody trying to divert your attention; by pointing out to dirt or waste on your person, spitting betel nut on you or throwing some money on the street.
- Keep your valuables or money safely tucked away inaccessibly on your person while traveling in public transportations. If you carrying them in a bag, keep the bag close to your person in front of you.
- Do not respond to people offering to assist or sexual advances in public transportations. These are some of the common diversionary tactics employed.
- The safest will be to avoid traveling in crowded transportations while carrying heavy cash or valuables.

Servant Verification

- The city police provide a free service to the public. Whenever you are engaging the services of Domestic Servants like Maid, Caretaker, Cook, Driver, Office Boy or Watchman you can approach the local station for verifying their antecedents.

Vehicle Safety

- While going shopping or anywhere please park your vehicles in the vehicles parking lot.
- **Don’t keep vehicles in your house compound without locking, during the night hours don't park your vehicles out side your compound wall.**
- If your vehicle is equipped with an alarm set it every time you exit the vehicle.

- In case your vehicle is stolen, please inform the local police station as early as possible. The delay in informing will result in more crimes being committed and increase the difficulty in tracing the vehicle.
- If you notice an unattended and unknown vehicle parked for a day or more, inform the local police, beat constables or **CONTROL ROOM**
- When buying a used vehicle, compare the Registration number, Engine number and Chassis number with the RC book. Checkup with database of lost and found vehicle in this website.
- **Try to park where there are lots of people passing, good lightning and CCTV.**

Shops /Banks

- Bankers, Jewelers and shop owners are advised to fix Burglar alarm, CCTV and engage young and healthy watchmen after checking their antecedents.
- Get trained in detecting fake credit cards and counterfeit.
- Banks are advised to install hot lines with the local police stations.
- The frontage should be well lit after business hours. Do not allow tramps, paper pickers and beggars to sleep in the shop front.
- New type of Shutters (Single Piece) cannot be easily breached.

Senior Citizens

- Inform the local police station if Senior citizens are home alone for a considerable period of time.
- They are advised to exercise precaution in interacting with or taking assistance from strangers.
- Remember to call **CONTROL ROOM**

Women

- **Awareness :** The first, and probably most important, component in self-defence is awareness: awareness of yourself, your surroundings, and your potential attacker's likely strategies.
- **Use your sixth sense**:"Sixth sense" "Gut instinct" Whatever you call it, your intuition is a powerful subconscious insight into situations and people. All of us, especially women, have this gift, but very few of us pay attention to it. Learn to trust this power and use it to your full advantage. Avoid a person or a situation which does not "feel" safe–you're probably right.
- Be alert when you are carrying a purse on the street or in a store. Use a shoulder strap model and keep it tucked between your body and your arm. Do not dangle a purse by the straps or hold a clutch-style purse just in the hand

Children

- Teach your child to tell your name, house address and contact numbers, which will be very useful if they get lost.
- But advise them not to pass on this information to casual enquirers or over phone.
- Don't leave children alone in crowded places. For toddlers who are yet to communicate clearly, tie an identity tag/card.
- Train the children not to accept eatables from strangers, not to accompany strangers who call them on some pretext.
- Remember an exclusive **WOMEN/CHILD HELPLINE** is available in all the districts

Travelling

- Ensure the luggage is latched and locked.
- Secure your luggage with a chain lock. Do not leave them unattended.
- Do not accept eatables from co-travelers.
- Do not reveal too many personal details to strangers.
- Don't wear heavy ornaments while travelling alone.
- Don't open your bag-containing valuable like cash and ornaments, while travelling in public places.

Walkers

- Early morning walkers are advised to avoid wearing valuable jewels, which will attract the snatchers.
- Please avoid walking in the dark, especially in lonely stretches.
- It's advisable for women to avoid lonely stretches even during daytime.

Job Rackets

- Be wary of advertisements or individuals offering overseas jobs. Check their antecedents.
- Check the website of the companies in which jobs are promised.
- If needed do not hesitate to approach the consulate of the country.

- For emergency complaints contact the **CONTROL ROOM**

How To Avoid Identity Theft

Identity Theft is a recent phenomenon. Globally, over 500,000 people are victims of this crime each year. The best protection always is prevention. Here are some tips to safeguard your good name:

- BEWARE Any document that has personal financial information on it can give an identity thief a foothold into your life.
- Put the charge slip copies in a safe spot until your credit card bills arrive.
- After you've reconciled your bill, shred every statement, including credit card receipts, old bank statements, medical statements, everyday bills and pre-approved credit card offers.
- Write clearly on all credit applications. Consistently and completely fill in all credit and loan applications using your full name, first, middle and last. Every bill that comes to your house should be addressed exactly the same.
- Monitor your credit accounts carefully, so you'll know if a bill's missing or unauthorised purchases have been made.
- Close out unused credit cards. Cutting them up is not enough.
- Limit the number of credit cards you carry. The fewer cards you have, the easier it is to track them.
- If you're moving, contact all your creditors and update them of your address changes immediately. You don't want credit information and new credit cards being delivered to the wrong address.
- If your credit card expires and you don't receive a new one, call your creditor immediately.
- Don't provide your credit card number to anyone who contacts you through telephone solicitation.
- Make sure any online credit card charges are handled through a secure site or in an encrypted mode. You'll know you're on a secure site if the web page on which you conduct your transaction begins with '**https**' instead of the usual 'http'.
- Only shop on websites that offer a privacy policy. Know how your personal information will be handled. Print out privacy policies, warranties, price guarantees and other important information.
- Be watchful of shoulder-surfers. At ATMs and phone booths, thieves will stand close enough to see PIN numbers punched in by users.