GUIDELINES FOR PUBLIC

The following guidelines and safety Tips for Senior Citizen Safety

1. Majority of the offences committed by the persons are known to the victim's - servant, watchman, craftsman etc.
2. Database of elderly people staying alone in the jurisdictions of various Police Stations is generally incomplete due to poor response.
3. Servant's information is not provided to Police.

DO'S AND DON'TS FOR CITIZEN

Senior Citizen can employ a servant after verifying his real name, native address with the help of the nearest Police Station or through the security wardens

1. Never discuss financial matters in front of your servant.
2. It is always safe to deposit your valuables in safe deposit vault of any Bank.
3. Treat your servant in a humane way.
4. Do not allow any of the relatives or friends of your servant to visit your house. If at all he has any frequent visitor, get his antecedents checked from police and try to keep the number of such persons.
5. Make your neighbour know of you being staying alone. The Housing Society also needs to know this.
6. Use of modern security gadgets is always advantageous. Door alarm, electronic eye bell etc. is available in market.
7. Install a peephole in your front door and always check the identification of strangers before you let them inside your home.
8. Never leave spare keys in open or in the conventional hiding places.
9. Verify the identity of any repairman. Use the telephone number listed in the phone book.
10. Inform your society about the unacquainted visitors, so that their identity could be checked at the entrance gate of the society.
11. A well-designed electronic alarm system attached to the office of your Housing-Society or to the watchman’s cabin would be advisable so as to send alarm signals to all simultaneously.
12. When you admit a workman or a salesman, do not leave him alone at any time.

The Guidelines for Cyber Safety

1. Cyber security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks.
2. Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.
3. Though, cyber security is important for network, data and application security.
4. Communication security-protecting organization communication media, technology, and content.
5. Network security-is the protection of networking components, connection and content.
6. Information security-protection of information and its critical elements, including the systems and hardware that use, store or transmit that information.

Cyber Crime

1. The former descriptions were "computer crime", "computer-related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime were added to the definition. Also, Internet brought other new terms, like "cybercrime" and "net" crime.
2. Other forms include "digital", "electronic", "virtual", "IT", "high-tech" and technology-enabled" crime.
3. It is a criminal activity committed on the internet.
4. Cyber Crime-Where computer is either a tool or target or both.

Cyber Crimes Includes:-

1. Illegal access.
2. Illegal Interception.
3. System Interference.
4. Data Interference.
5. Misuse of devices.
6. Fraud.

Advantage of cyber security:-

1. It will defend from hacks and virus.
2. The application of cyber security used in our PC needs update every week.

3. The security developers will update their database every week once. Hence the new virus also deleted.

Safety Measures:-

1. Read Privacy policy carefully when you submit the data through internet.
2. Encryption: lots of website uses SSL (secure socket layer)to encrypt a data.
3. Disable remote connectivity.
4. Use antivirus software.Ensure that your virus definitions are up to date and run anti-virus.
5. Install and use a firewall, pop-up blocker.
6. Assignment of computer to a particular person with password protection in offices. Install the firewall and maintain the logs of firewall. Preservation of evidence (logs/received emails in question etc.) Disconnect from internet when not in use.
7. Habitually download security protection update patches & Keep your browser and operating system up to date. Never share photographs in compromise positions. Make the wireless network invisible by disabling identifier broadcasting. Encrypt the network traffic.
8. Change administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.
9. Uninstall unnecessary software.
10. Make Backups of Important Files and Folders to protect important files and records on your computer if your computer malfunctions or is destroyed by a successful attacker.
11. Check security settings.
12. Use secure connection.
13. Open attachments carefully.
14. Use strong passwords- Easy to remember and difficult to guess type password. Use alphanumeric and special characters in your password. The length of password should be as long as possible (More than 8 characters).
15. Be extremely wary of spam legitimate looking email asking for confidential information. Never ever click on the link given in the spam email. Always delete spam emails immediately and empty the trash box to prevent accidental clicking on the same link.
16. Beware of promises to make fast profits. Be cautious of exaggerated claims of possible earnings or profits. Beware of lotteries that charge a fee prior to delivery of your prize. Contact the actual business that supposedly sent the email to verify if the email is genuine. Beware of references given by the promoter.

17. Don’t give personal information to anyone unless required.
18. The only system which is truly secure is one which is switched off and unplugged.
19. So, only way to be safe is Pay attention and Act smart.

New Age Cyber Crimes:-

1. Credit card frauds.
2. Cyber pornography.
3. Sale of illegal articles- narcotics, weapons, wildlife.
4. Online gambling.
5. Intellectual Property crimes- software piracy, copyright infringement, trademarks violations, theft of computer source code.
6. Email spoofing.
7. Forgery.
8. Defamation.
9. Cyber stalking (Section 509 IPC)
10. Phising.
11. Cyber terrorism.

Other Types of Cyber Crimes:-

1. Hacking.
2. Information Theft.
3. E-Mail bombing.
4. Salami attacks- web jacking.
5. Denial of service attacks.
6. Trojan attacks.

Training in New Age Crimes:-

1. Awareness about different Cyber crimes by organizing workshops and training programmes.
2. Use of VPN (Virtual Private Network).
3. Knowledge of Dark Web- TOR Browser etc.

The following DO’s & DON’T’s for ATM/Credit Usage

DO’s:-

1. Install and use a firewall, Pop-up blocker and spyware detector. Ensure that your virus definitions are up to date and run anti-virus and spyware detector/cleaners regularly.
2. Make Backups of Important Files and Folders to protest important files and records on your computer if your computer malfunctions or is destroyed by a successful attacker?
3. Use strong passwords- Easy to remember and difficult to guess type password. Use alphanumeric and special characters in your password. The length of password should be as long as possible (More than 8 characters).
4. Assignment of computer a particular person with password protection in offices. Install the firewall and maintain the logs of firewall. Preservation of evidence (logs/received emails in question etc). Disconnect from internet when not in use.
5. Habitually download security protection update patches& Keep your browser and operating system up to date. Never share photographs in compromise positions. Make the wireless network invisible by disabling identifier broadcasting. Encrypt the network traffic.
6. Change administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.
7. Disable file sharing on computers. Turn off the network during extended periods of non-use, etc.
8. Avoid online banking, shopping, entering credit card details, etc if network is not properly secured.
9. Check your online account frequently and make sure all listed transactions are valid Use a variety of passwords, not same for all of your account.
10. Be extremely wary of spam legitimate looking email asking for confidential information. Never ever click on the link given in the spam email. Always delete spam emails immediately ad empty the trash box to prevent accidental clicking on the same link.
11. Be wary of website that require your card details up font before you actually place an order. Not to believe everything you read online. Take your time- do not rush into things.
12. Avoid posting your cell phone number online. Never respond to text messages from someone you don't know use your cell phone.
13. Open email attachment carefully, be careful while downloading any free software or screensaver etc. Not delete email in question, save the email and take out the full header of the email and report the crime. Be cautions when dealing with individuals outside of your own country. Be cautious of unsolicited offers. Never purchase anything advertised through an unsolicited email.

14. Beware of promises to make fast profits. Be cautious of exaggerated claims of possible earnings or profits. Beware of lotteries that charge a fee prior to delivery of your prize. Contact the actual business that supposedly sent the email to verify if the email is genuine .Beware of references given by the promoter.
15. Ensure you understand all terms and conditions of any agreement. Be leery when the job posting claims "no experience necessary". Always type in the website addresses yourself rather than clicking on a provided.

DON'T's:-

1. Your real name, home address your phone number your friends' or family members' private information. Your passwords
2. Don't Expose yourself that you are not available in town or give your details about location and itinerary when email auto responder enabled. Hand over your credit card to any person.
3. Auto-connect to open Wi-Fi (wireless fidelity) networks. Get confused, frightened or pressured into divulging information if you receive an e-mail purporting to be from your bank or credit card provider as criminal use scare tactics. Keep passwords stored on your computer.
4. To go online without virus protection and a firewall in place. Open email attachment if you are not sure about it. Assume a company is legitimate based on "appearance'' of the website. Be wary of investments that offer high returns at little or no risk.
5. Do not Share details like Credit/Debit Card number, CVV&OTP to unknown people and unverified websites and tele-calling persons.
6. Do not write PIN on your credit/Debit Card.
7. Do not take help form unknown people while using ATM Card
8. Try to avoid using ATM Without security guards
9. Do not allow anyone to carry your ATM Card away from eyes.
10. Do not share your personal information on Social Media site like Facebook, Twitter, Instagram etc.
11. Don't except friend request from unknown sources.
12. Don't install free wares from untrusted websites.
13. Don't download pornographic material on your mobile phone and Laptop/Desktop.
14. Do not post your family and personal pictures on social Media. And don't make them public.
15. Don't' get into trap of fake calls like winning lottery, blocked credit/Debit Card, Bonus on Investment/ Insurance policies, jobs etc.

The following are the guidelines/ Safety Tips for various types Disasters

(a) भूकम्प (Earthquake)

1. अपने घर को भूकम्परोधी बनाएँ, भारी फर्नीचर व वस्तुओं को सुरक्षित स्थानों पर रखें।
2. अपने घर के आसपास एक ऐसे स्थान का चयन करें, जहाँ भूकम्प के दौरान तथा उसके बाद सुरक्षित शरण ली जा सके।
3. घर छोड़ते वक्त अपना आपातकालीन किट लेना न भूलें, जिसमें जीवन रक्षक दवाओं के साथ कम से कम तीन दिनों के लिए खाद्य सामग्री व पानी शामिल हो।
4. भूकम्प के दौरान किसी मजबूत फर्नीचर के नीचे छुप जाएँ तथा अपने सिर व शरीर के महत्वपूर्ण हिस्सों को ढक लें। इस दौरान फर्नीचर को पकड़कर रखें।
5. काँच व खिड़कियों से दूर रहें तथा भूकम्प के झटकों के दौरान इमारत से बाहर न निकलें।
6. अगर घर से बाहर हैं तो शीघ्र खुले मैदान अथवा सुरक्षित शरण स्थल पर चले जाएँ, इमारतों, पूलों व बिजली के खम्बों से दूर रहें।
7. सावधानीपूर्वक बाहर जायें और अपने आसपास एवं ऊपर अस्थिर चीजों एवं खतरों की जांच करें। कि आपके आसपास या आपके ऊपर कोई अन्य खतरा तो नही है। यह भी देखें कि आपको कोई चोट तो नहीं लगी है।
8. यदि भूकंप का झटका एक मिनट व उससे अधिक समय तक के लिए रहे, तो अगले आने वाले झटकों के लिए भी तैयार रहें।
9. क्षतिग्रस्त भवनों से अपने आपको दूर रखें। सुरक्षा के निर्देषों की जानकारी के लिए स्थानीय टीवी देखें या रेडियों सुनें।

(b)बाढ (Flood)

1. यदि आपके क्षेत्र में बाढ़ की आषंका है तो स्थिति से निपटने के लिए वैकल्पिक निर्माण सामग्री पर विचार करें।
2. रेड़ियो या टीवी से बाढ़ की सूचना लगातार लेते रहें।

3. अपने निकटतम शरण स्थलों व सुरक्षित मार्गों की पूर्ण जानकारी रखें। आपातकालीन किट तैयार रखें।
4. आपात्कालीन स्थितियों से निपटने के लिए पर्याप्त मात्रा में खाद्य पदार्थ, पीने का पानी आदि का भंडारण कर लें। उबला पानी पीयें/हल्का खाना लें, उपलब्ध भोजन/खाद्य सामग्रियों को ढक कर रखें।
5. बच्चों, बुजुर्गों, गर्भवती महिलाओं को खाली पेट न रहने दें।
6. बिड्ढधर प्राणियों से सचेत रहें।
7. गर्म कपड़े, आवष्यक दवाएँ, कीमती सामान, जरूरी कागजात आदि सुरक्षित बैग में पैक रखें। आपात स्थिति में इसे सदैव अपने साथ रखें।
8. फर्नीचर, कपड़े और कीमती सामान, बेड, टेबल आदि जैसे ऊँचें स्थानों पर ही रखें।
9. मुख्य बिजली की आपूर्ति बंद रखें। उन बिजली उपकरणों का प्रयोग न करें जो पानी में भीगे हों।
10. बच्चों को बाढ़ के पानी के पास खेलने की अनुमति ना दें।
11. पानी की गहराई और धारा का अनुमान न हो तो बाढ़ के पानी में कदापि न जायें।

(c)भूस्खलन(Landslide)

1. ढलान, पहाड़ी सिरों के किनारे, जल निकासी के पास या प्राकृतिक कटाव वाली घाटियों के पास घर बनाने से बचें।
2. यथाशीघ्र भूस्खलन के क्षेत्र से दूर चले जायें।
3. अपने आसपास की जमीन में होने वाले परिवर्तनों का ध्यान रखें।
4. सतर्क और जागृत रहें, कई लागों की मृत्यु भूस्खलन के दौरान सोते रहने से होती है।
5. असामान्य आवाज से सतर्क रहें, जैसे पेड़ के टूटने या चटकने, पत्थरों के टकराने की आवाज इत्यादि भूस्खलन का संकेत हो सकती है।
6. भूस्खलन के दौरान नदी घाटियों और निचले इलाकों से दूर रहें।
7. यदि आप एक नदी या जल स्त्रोत के पास हैं तो जल स्तर में हुई अचानक वृद्वि या पानी के प्रवाह में हुई कमी से सतर्क रहें। पानी का अचानक गंदा/मैला हो जाना, भूस्खलन आने का संकेत हो सकता है।

8. अपने निकटतम शरण स्थल पर आश्रय लें ताकि आप भूस्खलन से सुरक्षित रहें।
9. अगर आपको जगह खाली करने के लिए निर्देशित किया गया हो तो एक नामित सार्वजनिक आश्रय के लिए प्रस्थान करें।
10. भूस्खलन के क्षेत्र से दूर रहें, वहाँ अतिरिक्त भूस्खलन होने का खतरा हो सकता है।
11. भूस्खलन क्षेत्र में प्रवेश किए बिना घायल और फंसे व्यक्तियों की जाँच करें तथा बचाव दल को उनके स्थान के लिए निर्देशित करें।

(d)जंगल की आग(Forest fire)

1. जंगलों में गर्मी के मौसम के दौरान सूखे कूड़े को एकत्र न होने दें।
2. आग के चारों ओर खुदाई या पानी द्वारा घेरा बनाने का प्रयास करें, यदि संभव नहीं हो तो अग्निशमन कर्मियों को बुलाएँ।
3. आग के दौरान अग्रिम जानकारी के लिए नियमित रूप से रेडियों सुनें और आवश्यक निर्देशों एवं सलाह का पालन करें।
4. जंगल में अचानक आग से डरें नहीं, शांत रहें, धैर्य रखें, समुदाय को समस्या पर धैर्य से काबू पाने के लिए प्रोत्साहित करें।
5. सुलगती हुई सिगरेट, बीड़ी इत्यादि जंगल में ना फेंके।
6. जंगल या उसके आसपास जलती लकड़ी इत्यादि ना छोड़ें।
7. आग के दौरान जंगल में प्रवेश ना करें।
8. जंगल या आसपास पिकनिक के दौरान भोजन बनाने के पश्चात आग को पूर्णरूप से बुझा दें।

(e)तीव्र गर्जन एवं बिजली गिरना (Rapid roaring and lightning fall)

1. याद रखें, रबर सोल के जूते एवं रबर-टायर बिजली गिरने से कोई सुरक्षा प्रदान नहीं करते हैं।
2. संभावित आपदा से पूर्व, घर के सभी बिजली उपकरणों का प्लग से सम्पर्क हटा दें, ताकि आपदा के दौरान करंट से उपकरणों को बचाया जा सके।

3. बिजली के उपकरणों या तार के साथ संपर्क से बचें। अन्य बिजली के उपकरणों को बिजली के संपर्क से हटा दें। कंक्रीट के फर्श पर न लेटे और कंक्रीट की दीवारों का सहारा न लें। बिजली गिरने के दौरान इनमें करंट का प्रवाह हो सकता है।
4. स्थानीय रेडियो व अन्य संचार साधनों के द्वारा मौसम की जानकारी व अन्य निर्देश प्राप्त करते रहना चाहिए।
5. बिजली के खंभों/टूटे तारों से दूर रहें व इसकी जानकारी नजदीकी बिजली कार्यालय अथवा पुलिस चौकी को शीघ्र दें।

Guidelines for Safe Neighbourhood:-

1. Remove throw away papers from your doorstep during your absence.
2. Rearrange the positions of interior draperies from time to time.
3. Notify the police if they detect anything suspicious stranger around the house, enquiring strangers: etc.

Safety of Women & children

(a)PERSONAL SAFETY TIPS FOR WOMEN AT HOME:-

1. Women who live alone should list only their last names and initials on their mailboxes and in the telephone directory.
2. Always keep the door locked, even if you are at home and even if you leave the house for just a few minutes.
3. Never open the door automatically after a knock, Ensure that strangers have identified themselves properly before allowing them to enter, Utilize a peep-hole (magic-eye) to verify identification.
4. Leave the light on over the door which you will be using to enter at night. Have your key ready so that the door may be opened immediately.
5. Close curtains at night.
6. Never admit over the phone or to strangers that you will be alone at home.
7. Lifts: If you live in an apartment building where you know most of the residents and find your self in the lobby with a stranger, let him take the lift first and wait for it to return for you. If you are on the lift and someone’s presence makes you uneasy, get the control panel. If someone attacks, hit the alarm button and press as many buttons as you can so that lift will stop at any of several floors.

8. If a stranger requests the use of your phone, do not let him enter your apartment. Place the call for him instead.
9. If you return home and detect evidence that someone as broken in to your domicile, do not enter the premises and do not scream. Proceed to the closest neighbor's house and phone and police from there.

(b)FOR FREQUENT FEMALE TRAVELERS:-

1. The above recommendations apply to men and women equally. However a few additional suggestions are advisory for women.
2. Travel on well-lit streets and keep your purse out of sight.
3. If you have car trouble in a dark area, lock yourself in and await the arrival of the police.
4. If a stranger stops to give you assistance do not get out of the car.
5. Ask the person to call for help.
6. Do not stop & offer help to stranded motorist.
7. If you suspect that someone is following you, drive to the police station or police picket.
8. Women are urged not to ask for lift under any circumstances.
9. Never pick up a person asking for lift.

DO'S & DON'T's for children:-

1. Never run errands for strangers, even for money.
2. Never accept candy money or gifts from a stranger, or an invitation to a movie, etc.
3. Never get in to a car with a stranger for any reason.
4. Never Hitch-Hike.
5. If a stranger attempts to coax you into a car, yell and run, then write down the license number from a safe distance, or scratch it in the dirt. Then tell your parents teacher or a policemen.
6. If a friend gets in to a car with a stranger, even if you have warned him not to, write down the license number and tell a policeman, your parents or teacher right away.
7. Make sure that your parents always know you are and who you are with.
8. When collecting for charities, always travel in groups of two or more, and never go inside a stranger's house.
9. Teach your children their full names, address and telephone No. Tell them never to admit to being home alone on the phone or to someone at the door.

10. Tell them never to admit to being home alone on the phone or to someone at the door.
11. Instruct children to look out for each other and tell you when something unusual or suspicious happens.
12. Report suspicious individuals or vehicles lurking in areas where children play to the police.
13. Ask a trusted neighbor to provide sanctuary for your children should any threat or emergency arise while you are away from home. Offer to do same for them.
14. Every child should know that police are friends be able to recognize the uniform and know that a policeman will be receptive if the child is lost or frightened.
15. Children should be encouraged to play with friends and never in isolated areas or vacant buildings.
16. Parents should always know where their children are.
17. Parents should ensure that baby-sitters are known and can be trusted.

Kidnapping And Hostage Survival - Some Do's & Dont's At Residence & Office:-

1. Secure perimeter of the house/office.
2. Trim bushes and trees around as these could block the view towards outside.
3. As far as possible,use only one door and lock the rest from inside. However always provide for an escape door.
4. Keep important telephone numbers of the nearest police stations, police control room, known police officer's and helpful neighbours handy near the telephone.
5. Visitors in the office must always be escorted by the security staff who should remain present until greetings have been exchanged.
6. Encourage your friends to telephone prior to an intended visit, this reduces the number of unexpected callers to the minimum.
7. Keep a watch dog at the residence.
8. Open the front door only after checking the identity of the visitor through a peeping eye.
9. Check all the doors and windows every night before retiring to ensure that they are properly locked/bolted from inside.
10. Keep a light burning in the front door area during the jhours of darkness.
11. Keep a strict check on the house/office keys. If the key is lost, have a new lock fitted.
12. Inform the police of the presence of suspicious vehicles or persons near the house or office.
13. Know your neighbours well enough so that normally you can watch each others houses.

14. Do not accept invitations on telephone to visit a place/person unless the identity of the caller is fully established.
15. Do not encourage servants bring their friends, relatives into the premises.
16. Ask the members of the household including servants / office staff not to disclose the whereabouts of the protected person and his future appointments to unidentified callers.
17. Treat late callers with suspicion and refuse admittance unless he/she is known to you.
18. Inform police at once in the event of any visitor attempting forcible entry. Remain for signs of any surveillance since terrorists generally keep a watch on potential victims for some time before striking.

While Travelling:-

1. Always be while leaving the gate of your house or returning to the house. This applies to entry and exit from the office complex as well. Keep your car doors locked while travelling/when parked in the garage.
2. If no garage is available, leave your car at a place where it can be seen by everyone.
3. Vary your time of departure and change your route frequently. Use alternative routes occasionally evenif this may involve increase in commuting time.
4. Occasionally, sit beside the driver in the front seat.
5. Travel in a group to the extent possible.
6. If you think you are being followed, take a known detour and if you are still suspicious, head for the nearest police station.
7. Avoid narrow lonely dark streets and keep to the well -lit main routes especially those that pass by police posts.
8. Beware of accident scenes or broken down vehicles they may be a decoy.
9. If something untowards appears to be taking place on the road ahead, stop and turn before it is too late.
10. Give details of your intended movements to only those who need to know.
11. Ensure that someone in your family knows your whereabouts.
12. While moving in a car, open the windows only enough for ventilation.
13. While traveling by train, enter into a compartment which is already occupied .
14. Extend all cooperation to personal security officers in carrying out their legitimate duties.
15. In case a taxi has to be engaged , avoid hiring the first one in the line or the one which seems to be waiting. Do not give any specific instruction to the driver about the route/destination before commencement of the journey.

Safety begins at home the door step code:-

1. Install an outside light above the front door so that you can see callers clearly after dark.
2. Use a door viewer and ask the caller's name every time you answer the door, do not open the door until you are sure who is there and that you to see him or her.
3. If the caller if a stranger, always use a door chain or limiter when you open the door.
4. If the caller claims to be an official public service employee, postman or even the police open the door with the chain in place and ask for proof of identity. Take your time examining any document and satisfy yourself that it is genuine.
5. If you are in any doubt, ask the person either to wait or to come back later so that you can ring the company he or she claims to represent for verification.
6. If the caller is abusive or suspicious ring 100, inform the police.
7. If a stranger asks to use your telephone in an emergency, offer to make the call yourself wile he waits out side.
8. If you think that some one is tying to break into your home at any time, ring the police.
9. Do not place advertisements in the newspaper or local shop window that would result in people calling at your, home when you might be there alone.
10. If your are trying to sell or rent your home, do not show prospective buyers or tenants around on your own.
11. Have a light on outside door when you return home after dark.
12. Keep garden plants trimmed so that they can not conceal an intruder.
13. As you approach your door have a good look in all directions before putting your key in the lock. Let yourself in promptly and lock the door behind you.
14. If there are signs of intrusion, do not go in.
15. Never hide keys outside.
16. Avoid lending keys to workmen.
17. Do not leave spare keys with the building porter unless you want to, you are not obligated to do so.
18. Replace the locks immediately if the keys to your home are lost or stolen.