Motor vehicle safety

- Park in well lighted areas, where your vehicle is visible; avoid parking next to vans or trucks.
- Keep all items out of sight, especially valuables. Remove or place CD players/cases, etc. in the trunk.
- Service your vehicle regularly to avoid breakdowns.
- Keep your vehicle locked at all times.
- Consider "The CLUB" or an alarm system.
- When leaving your car for service, remove your other keys.
- Have your key ready when you approach your car. Before getting in, check inside and under your car to make sure no one is hiding.

Safe walking, jogging or running

- Plan your route in advance and walk/jog/run in familiar areas.
- Go with a known companion if possible.
- Carry identification.
- Don't wear jewelry or carry cash.
- Avoid secluded or dimly lighted areas.
- Avoid going after dark.
- Always face the traffic.
- If you're being followed, cross the street or change directions; keep looking back, and get a good description of the person.
- If you're still being followed, go to the nearest house or business and call the police.
- Wear bright colors to improve your visibility.

- Change your route and schedule.
- Avoid bushes where a person could hide.
- Take a key with you; do not leave your house or room unlocked; someone could be watching to see when you are not home.
- Carry your cell phone, a whistle, or shrill alarm to summon help.
- Do not wear headphones/earphones for an IPod, etc.

If you are attacked

- Go with your instincts, but be realistic about your ability to fight off someone; your instinct may be to run, scream, kick, hit or bite
  .
- If a weapon is displayed, don't resist. Give up your property and save your life.
- Do what you are told and don't make any sudden moves.
- Try to remember as many details as possible and call the police as soon as possible.
- Your goal should be to escape safety and survive; cooperate if you think that resisting may lead to further harm.
- Remember every situation is different; you are the only one who can decide the appropriate course of action.
- Constantly play the "what if" game to think about what you would do in a particular threatening situation. This will help prepare you to respond instinctively when a threat is encountered.
- After an event, never feel guilty about what you did or did not do.

Cyber security

General Tips

- Set secure passwords and don't share them with anyone. Avoid using common words, phrases, or personal information and update regularly.

- Keep your operating system, browser, anti-virus and other critical software up to date. Security updates and patches are available for free from major companies.

- Verify the authenticity of requests from companies or individuals by contacting them directly. If you are being asked to provide personal information via email, you can independently contact the company directly to verify this request.

- Pay attention to the URLs of websites you visit. Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net) to deceive unsuspecting computer users.

Email

- Turn off the option to automatically download attachments.

- Save and scan any attachments before opening them. If you have to open an attachment before you can verify the source, take the following steps:
  - ✓ Be sure your anti-virus software is up to date.
  - ✓ Save the file to your computer or a disk.
  - ✓ Run an anti-virus scan using your computer's software.

Social Media, Video Games, Forums, Chat Sites and more.

- Limit the amount of personal information you post. Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your friend posts information about you, make sure the information is something that you are comfortable sharing with strangers.

- Take advantage of privacy and security settings. Use site settings to limit the information you share with the general public online.

- Be wary of strangers and cautious of potentially misleading or false information.

Mobile

- Only access the Internet over a secure network. Maintain the same vigilance you would on your computer with your mobile device.

- Be suspicious of unknown links or requests sent through email or text message. Do not click on unknown links or answer strange questions sent to your mobile device, regardless of who the sender appears to be.

- Download only trusted applications from reputable sources or marketplaces.

Protecting yourself from identity theft

- Destroy private records and statements. Destroy credit card statements, solicitations and other documents that contain any private information. Shred this paperwork using a "cross-cut" shredder so thieves can't find your data when they rummage through your garbage. Also, don't leave a paper trail; never leave ATM, credit card or gas station receipts behind.

- Secure your mail. Empty your mailbox quickly, lock it or get a P.O. Box so criminals don't have a chance to steal credit card offers. Never mail outgoing bill payments and checks from an unsecured mailbox, especially at home. They can be stolen from your mailbox and the payee's name erased with solvents. Mail them from the post office or another secure location.

- Safeguard your Social Security number. Never carry your card with you, or any other card that may have your number, like a health insurance card or school issued ID. Don't put your number on your checks; your SSN is the primary target for identity thieves because it gives them access to your credit report and bank accounts. There are very few entities that can actually demand your SSN – the Department of Motor Vehicles, for example. Also, SSNs are required for transactions involving taxes, so that means banks, brokerages, employers, and a few others also have a legitimate need for your SSN.

- Safeguard your computer. Protect your computer from viruses and spies. Use complicated passwords; frequently update antivirus software and spyware. Surf the Web cautiously. Shop only at trustworthy web sites and be wary of obscuresites or any site you've never used before.

- Know who you're dealing with. Whenever you are contacted, either by phone or email, by individuals identifying themselves as banks, credit card or e-commerce companies and asked for private identity or financial information, do not respond. Legitimate companies do not contact you and ask you to provide personal data such as PINs, user names and passwords or bank account information over the phone or Internet. If you think the request is legitimate, contact the company yourself by calling customer service using the number on your account statement or in the telephone book and confirm what you were told before revealing any of your personal data.

- Take your name off marketers' hit lists. In addition to the national Do Not Call Registry (1-888-382-1222 or https://www.donotcall.gov), you also can reduce credit card solicitations for five years by contacting an opt-out service run by the three major credit bureaus: (888) 5-OPT OUT or https://www.optoutprescreen.com. You'll need to provide your Social Security number as an identifier.

- Guard your personal information. Ask questions whenever anyone asks you for personal data. How will the information be used? Why must I provide this data? Ask anyone who does require your Social Security number, for instance, cell phone providers, what their privacy policy is and whether you can arrange for the organization not to share your information with anyone else.

- Monitor your credit report. Each year, obtain and thoroughly review your credit report from the three major credit bureaus; Equifax (800-685-1111), Experian(883-397-3742) and TransUnion (800-680-4213) or at https://www.annualcreditreport.com) to look for suspicious activity. If you spot something, alert your card company or the creditor immediately.

- Review your bank and credit card statements carefully. Look for unauthorized charges or withdrawals and report them immediately. Make sure you recognize the merchants, locations and purchases listed before paying the bill. If you don't need or use department store or bank-issued credit cards, consider closing the accounts.

- Keep track of your billing dates/cycles and follow up with creditors if you don't receive bills/statements on time.

- Use random letters and numbers for passwords; don't use your mother's maiden name, your birth date, your graduation date, your social security number or any other familiar letters or numbers that can be associated with you as passwords.

- Be aware of how ID thieves can get your information. They get information from businesses or other institutions by stealing records, bribing employees with access to records, hacking into computers, rummaging through trash, posing as a landlord, employer, or someone else who may have a legal right to the information, stealing credit and debit card numbers as your card is processed by using a special information storage device ("skimming"), stealing wallets and purses containing identification and credit or bank cards, stealing mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information or completing a "change of address form" to divert your mail to another location.

If your identity is stolen

- Contact the fraud departments of each of the three major credit bureaus. Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, along with a victim's statement asking that creditors call you before opening any new accounts or changing your existing accounts:

    1. Equifax To report fraud: 1-800-525-6285 (P.O. Box 740241, Atlanta, GA 30374-0241):

    2. Experian To report fraud: 1-888-EXPERIAN (397-3742) (P.O. Box 9532, Allen, TX 75013), and

    3. TransUnion To report fraud: 1-800-680-7289 (Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634)

- Contact the creditors for any accounts that have been tampered with or opened fraudulently. Speak with someone in the security/fraud department of each creditor, and follow up with a letter.

- If your Social Security number has been used illegally, contact the Social Security Fraud Hotline at 1-800-269-0271.

- File a report with police in the community where the identity theft took place. Get a copy of the police report in case the bank, credit-card company, or others need proof of the crime.

- Keep records of everything involved in your efforts to clear up fraud, including copies of written correspondence and records of telephone calls.

Computer scams

- Computer phishing is a crime. Phishers attempt to fraudulently acquire credit card details and other sensitive personal data via bogus emails or pop-up windows. It may look like a legitimate email from a legitimate institution, but beware of unsolicited requests for information.

- Financial or payment institutions will never request that you send them personal sensitive data via email or pop-up windows.

- If you receive a suspicious looking email from any bank, lending, or payment institution, it is best to delete and not respond. If, by coincidence, you have an account with the

entity mentioned in the email, call your legitimate institution using the number on your physical bill or via the telephone book or through telephone information.

- Do not call the number that may be listed in the bogus email and do not click on any link listed in the bogus email.

Dating safety

- Check out a first date or blind date with friends first. Better yet, go with other friends on your first date.
- Carry money for a taxi or public transportation in case your date is cut short; bring a cell phone also.
- Know what you want sexually and don't send mixed messages.
- Trust your instincts about situations to avoid.
- Be clear and responsible in your communications with others.
- Be forceful, firm, and assertive.
- If you go out with other friends, don't get separated; watch out for each other.
- Do not lose self-control or impair your judgment by the use or abuse of alcohol or drugs.
- "No" means "NO."
- If someone is unable to give consent it is called sexual assault or rape.
- Watch your drink. If you have to leave it unattended, pour it out and get another one.

If you are a victim of sexual assault or rape

- Seek help immediately. Do not feel guilty or try to forget what happened; it is a crime and should be reported.
- Get medical attention as soon as possible. Do not shower, wash or change clothing; valuable evidence could be destroyed.

- Seek counseling and support to deal with emotional trauma; the police will be able to assist with determining the best available resources.

- If you think you've been assaulted while under the influence of an unknown drug (GHB, etc.) seek help immediately. Try not to urinate before providing a urine sample and if possible collect any glasses that you drank from.

Online dating

- Never give personal information to people that you don't know (name, home address, phone number, etc.).

- If you decide to talk to someone on the phone don't give out your number; call them and use caller ID block.

- Use a nickname in chat rooms or message boards.

- Meet chat friends in public places and with other friends; take a cell phone with you.

- Never go to someone's room, apartment of house that you just met.

Active shooter

If you are involved in a situation where someone has entered the area and started shooting, the following are a list of actions that are recommended:

1. If possible exit the building/area immediately, but only if it can be done safely.
2. Notify anyone you may encounter to exit the building immediately.
3. Notify the police. Give the following information:
    a) Your name
    b) Your phone number
    c) Location of the incident (be as specific as possible)
    d) Number of shooters
    e) Identification of shooter
    f) Number of persons who may be involved
    g) Your location

If exiting the building/area is not possible, the following actions are recommended:

1. Go to the nearest room or office.
2. Close and lock or barricade the door.

3. If unable to lock the door, use a wedge device or heavy furniture to block the door; a belt or other objects may be able to wedge the door shut.
4. Cover the door windows.
5. Depending upon the shooters location, exit out the window quietly and quickly.
6. Stay low, move away from the door, keep quiet and act as if no one is in the room.
7. DO NOT answer the door.
8. Notify the Public Safety or Police.
9. Provide information as needed.
10. Wait for the Police to assist your exit from the building.
    a) Follow all instructions by police officers
    b) Police may not know if the shooter is hiding among you, therefore police may search you and your belongings and/or do other thing for everyone's safety.

If you are trapped with the shooter, you need to decide whether to:

1. Stay still and play dead.
2. Run for an exit in a zigzagging pattern, or
3. Attack the shooter.