## **Personal Safety Tips**

### **Know how to contact Campus Security or the Police**

- Know how to contact Public Safety or the Police
- Know the emergency telephone number for your campus Public Safety or Police department.
- Keep the emergency phone numbers near your phones (stickers, magnets, etc.).
- Program emergency phones numbers into your personal cell phone.
- Learn where the campus emergency telephones are located in the parking lots and learn how to use them.
- Ensure that you are subscribed to the campus mass notification system on campus.
- Participate in any campus emergency safety programs being offered.

#### Walking around campus

- Familiarize yourself with the layout of the campus. Survey the campus while classes are in session and after dark to see that academic buildings, walkways, facilities, and parking lots are adequately secured and well-lighted.
- Plan the safest route to your destination; choose well-lighted, busy pathways and streets.
- Share your class schedule with your parents and trusted friends and give them your telephone numbers.
- At night, stick to well-lighted areas whenever possible and avoid "short cuts" through isolated areas.
- Travel in groups and avoid going out alone at night.
- Use the campus escort services at night.
- If you are being followed, change direction and go to the nearest business or home; knock on the door, and request that someone call the Police.
- Note the description of the person following you.

- Walk near the curb and avoid shrubbery or other places of potential concealment.
- Tell a friend or roommate where you are going and what time you expect to return.
- Stay alert to your surroundings and the people around you.
- Carry your purse close to your body and keep a firm grip on it; carry your wallet in an inside coat pocket or your front pant pocket.
- Keep your keys separate from your purse or backpack.
- Don't overload yourself with bags or packages and avoid wearing shoes that restrict your movements.
- Walk with a confident stride; keep your head up and look around.
- If a motorist stops and asks for directions, keep your distance from the car.

#### Cyber security

- Never give your password to anyone.
- Change your password frequently.
- Do not allow others access to your email account.
- Monitor your access time; by keeping track of when and how long you were or a computer system, it will be obvious if someone has gained access to your account.
- Be wary of anonymous "re-mailers".
- Do not put personal information or photos on your web page and do not give personal information that can identify where you live to social networking sites.
- Never leave your computer/laptop unattended.
- Engrave markings on your computer.
- Shop online only with companies that you know; check with the Better Business Bureau if unsure.
- Use a secure browser that will encrypt or scramble purchase information or pay with a money order or check.
- Update your virus software regularly, or when new versions are available.

- Do not download files sent to you by strangers or click on hyperlinks from people you don't know.
- Make certain that all your personal information is deleted from your computer prior to disposing of it.

### Obscene and annoying phone calls

- Hang up as soon as you realize the nature of the call. Do not try to find out who the caller is, even if you think it is a friend playing a joke.
- Use your answering machine to screen calls. You can also record an obscene phone call with the memo feature on some answering machines.
- If the calls occur frequently, keep a log of exactly when the call was received and what both parties said. Describe the type of voice and note any background noises.
- Consider changing your phone number and depersonalizing your answering machine message.
- Consider purchasing a machine that requires an access code before your phone will ring. If the calls continue, contact Public Safety or the Police.

## Vandalism and graffiti

- Report all vandalism and graffiti immediately.
- In addition to being illegal and costly, much vandalism and graffiti may also be bias, hate or gang related.

# **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 that 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. 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 the College 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 obscure sites 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 <a href="https://www.donotcall.gov">https://www.donotcall.gov</a>), 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 <a href="https://www.optoutprescreen.com">https://www.optoutprescreen.com</a>. 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 <a href="https://www.annualcreditreport.com">https://www.annualcreditreport.com</a>) 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 Public Safety or the 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.

### **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.
- Never be drawn in to a gang rape situation.

#### 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; Public Safety or 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.

# Party safety

- Never leave your drink unattended.
- Never accept a drink from anyone but the server at the bar.

- Attend parties with friends and look out for one another.
- If you think your drink has been tampered with, let someone know and go directly to the hospital.
- Control your amount of drinking.
- -Never drink and drive; always have a Designated Driver!

### Helping a crime victim

- Don't blame or judge the victim.
- Let the victim know that you are sorry for what happened.
- Offer the support of a professional counselor.
- Tend to the immediate physical or emotional needs of the victim.
- Do not disturb any crime scenes.
- Offer to support the victim if they decide to contact the police.
- Listen to the victim if they are willing to talk about the crime.
- Help with transportation, babysitting, cooking or other everyday needs.
- Offer to accompany the victim to the police station, hospital or courts.
- Tell the victim you will continue to be there for support and follow up with him/her later.

## Helping a crime victim

- Don't blame or judge the victim.
- Let the victim know that you are sorry for what happened.
- Offer the support of a professional counselor.

- Tend to the immediate physical or emotional needs of the victim.
- Do not disturb any crime scenes.
- Offer to support the victim if they decide to contact the police.
- Listen to the victim if they are willing to talk about the crime.
- Help with transportation, babysitting, cooking or other everyday needs.
- Offer to accompany the victim to the police station, hospital or courts.
- Tell the victim you will continue to be there for support and follow up with him/her later.