



TRAVEL SAFETY AND SECURITY

SDPD Crime Prevention

September 22, 2017

CONTENTS

PERSONAL SAFETY AND SECURITY

[When Away from Home](#)

[In a Hotel or Motel](#)

[When Using an ATM](#)

[While Driving](#)

[In Parking Lots, Garages, and Other Places](#)

[Before Going on a Trip](#)

[Passports](#)

[On a Cruise](#)

[Avoiding Trouble in a Foreign Country](#)

PROPERTY SECURITY

[Protecting Your Home and Property When You Are Away](#)

[Credit Freeze and Use of Credit Cards](#)

[At a Hotel or Motel](#)

[On a Train](#)

[When Out and About](#)

[What to Do If Your Purse or Wallet is Lost or Stolen](#)

[Using Wi-Fi, Laptops, and Mobile Devices in Public Places](#)

[Preventing Vehicle Break-Ins](#)

[Preventing Thefts of Parked Vehicles](#)

[Preventing Thefts from Vehicles](#)

The tips in this paper will help you protect yourself and your property when you are traveling away from home. Additional tips on home security, vehicle security, and preventing fraud and identity theft are available on the SDPD website at www.sandiego.gov/police/services/prevention/tips.

PERSONAL SAFETY AND SECURITY

When Away from Home

- Travel with a friend or in a group when possible. There is safety in numbers.
- Avoid traveling alone, especially after dark.
- Stay sober. Don't let alcohol impair your judgment. Only drink beverages you have seen prepared. Ask that bottled drinks be served unopened. Don't leave your drinks unattended. Someone could slip a drug into one that causes amnesia and sleep.

- Plan your touring. Don't discuss your plans with strangers. Beware of strangers who seem overly anxious to help you. Select guides carefully.
- Get good directions to avoid getting lost.
- Find an open business to get directions if you get lost. Don't appear to be lost by stopping and looking at addresses or street signs.
- Stick to well-lighted main streets and public areas. Avoid areas where your personal safety may be at risk. If someone does grab you, make a scene: yell, kick, and try to get away.
- Leave your itinerary with a friend or relative and check in with them periodically.
- Keep track of time and don't be late for appointments or meetings.
- Shop with a friend when possible.
- Don't buy things from people on the street who offer you a great deal, especially if you have to follow them somewhere to get it.
- Don't fight for your purse if someone tries to take it by force.
- Only use authorized taxis. You could be overcharge, robbed, or kidnapped when using "gypsy" taxis. Before getting into a taxi write down its number and the driver's name.
- If you are arrested for any reason, ask to notify the nearest U.S. Embassy or Consulate.

In a Hotel or Motel

- If the desk clerk says your room number aloud when you check in, ask for a different room and have the number written on your keycard sleeve and discreetly handed to you.
- Avoid rooms with ground-floor windows or sliding-glass doors to pools or beach areas.
- If you feel uncomfortable walking to your room alone, ask the desk clerk to provide an escort.
- Determine the most direct route to and from your room, to fire escapes, stairs, elevators, and phones. Count the number of doors between your room and the exits in case you need to escape in smoke or darkness.
- Keep your door locked when you are in your room. Use both the deadbolt lock and the security bar/chain.
- Keep your windows locked, and blinds and drapes closed for privacy.
- Be sure that sliding glass doors and doors to connecting rooms are locked.
- Safeguard your room key or card at all times.
- Destroy your room card after your stay. Some may be encrypted with your credit card information.
- Use the peephole in the door to identify anyone requesting entry. Open the door only if you are certain it is safe to do so.
- Don't invite strangers into your room.
- If you are worried about being spied on through the peephole in the door cover it with a piece of opaque tape.
- If you haven't requested room service or housekeeping and someone knocks on your door claiming to be a staff member, call the front desk to verify the claim before opening the door.
- If you receive a call about an emergency that requires you to leave your room, hang up and call the front desk to verify it.
- If you receive a call asking for your credit card number to verify a room charge, hang up. It's probably a scam. Call the front desk to see if there's any problem with your account.
- Report any suspicious persons or activities to the front desk.
- Don't stay in a ground-floor room or rooms near stairwells or elevators, especially if you are a woman and traveling alone.

- Don't leave anything on your door knob to indicate that you are not in your room. Call housekeeping to request maid service. Call room service to order food.
- Use valet parking if the garage is dimly lit or the neighborhood has a high crime rate.
- Ask your hotel concierge or desk clerk about dangerous areas and avoid them. Neighborhoods can change a new threats may have emerged since the last time you visited or the guidebook you're using was printed.
- When you go out tell the hotel manager when you expect to return and who to call if you're not back by then.
- Carry a card with your hotel's name, address, and phone number.

When Using an ATM

- Use ATMs that are inside a store or a bank. If you use an outside ATM, it should be well-lighted, in a busy area, under video surveillance, and have clear lines of sight in all directions, i.e., there should be no nearby building corners, shrubs, signs, etc. that could provide possible hiding places for an attacker.
- Get off your cell phone and be alert when using an ATM.
- Be aware of your surroundings before and during your transaction, especially between dusk and dawn. Return later or use an ATM in a store or bank if you notice anything suspicious, e.g., a person loitering nearby.
- Complete your transaction as fast as possible and leave the facility.
- Don't go alone.
- Park in a well-lighted area as close to the ATM as possible.
- Keep your doors locked and passenger and rear windows rolled up when using a drive-through ATM.
- Put your cash, receipt, and ATM card away promptly. Count your cash later in private. Do not leave your receipt at the ATM site.
- Avoid being too regular. Don't use the same ATM at the same time of day and day of the week.
- Make sure you are not being followed when you leave an ATM location. Drive immediately to a police or fire station, or any well-lighted and crowded location or open business and get help if you are being followed. Flash your lights and sound your horn to attract attention.
- Give up your money or valuables if you are confronted by an armed robber. Any delay can make a robber more nervous and increases the likelihood of violence.

While Driving

- Keep your doors locked and your windows closed.
- Know where you are going. Stop and get directions before you get lost.
- Avoid driving alone, especially at night and in dangerous areas.
- Never pick up hitchhikers.
- Drive to the nearest open business and call the police if anyone is following you. Don't go home. The number to call is **911** in the United States and some other countries. You should get the numbers of the places you'll be going to before you leave as suggested below.
- Keep your vehicle in gear when stopped for traffic signals or signs. Try to leave room to drive away if threatened. Be alert for anyone approaching your vehicle.
- Keep purses and other valuables out of view when driving alone. Put them in the trunk or on the floor.

- Honk your horn or flash your emergency lights to attract attention if you are threatened while in your vehicle.
- Stay in your vehicle if you stop to aid others. Find out what the problem is and offer to call or drive to the nearest phone and report the situation.
- Keep your vehicle in good mechanical condition so it won't break down and leave you stranded on the road. Also keep enough gas in the tank so you won't run out.
- If your vehicle breaks down or runs out of gas, pull over to the right as far as possible, raise the hood, and call or wait for help. Remain in your vehicle with the doors and windows locked until you can identify any person who comes to help.
- Be wary of minor rear-end collisions, especially at night on dark freeway off-ramps. Remain in your vehicle with the doors and windows locked if you are uneasy or suspicious. Drive to the nearest open business to check the damage and exchange insurance information.
- Control your gestures and other reactions to keep "road-rage" incidents from escalating to violence.

In Parking Lots, Garages, and Other Places

- Park in open, well-lighted, and populated areas near your destination. Park in a garage where you don't have to use stairs or elevators.
- Never park next to trucks, vans, dumpsters, and other objects that obstruct visibility and provide hiding places. Check that no one is hiding around your vehicle before you get out.
- Avoid parking or walking near strangers loitering or sitting in vehicles.
- Have someone escort you to your vehicle if you are concerned about your safety and are uncomfortable about walking alone. Or wait until there are more people around.
- Remember where you parked so you can return directly to your vehicle. Be alert and walk purposefully.
- Don't overload your arms with packages. Use a cart or make another trip.
- Be aware of your surroundings and the people around you. Don't be distracted while walking to your vehicle. This includes fumbling with your purse or packages, looking for keys, and using a cell phone. Have the key in hand when you approach your vehicle so you can open the door immediately.
- Check that no one is hiding in or around your vehicle before you get in.
- If a van has parked next to your vehicle, enter it on the other side.
- Lock the doors immediately after getting in your vehicle.
- Don't resist or argue with a person who wants to steal your vehicle. Your life is much more valuable than your vehicle. Be especially alert when parking at fast food places, gas stations, ATMs, and shopping areas along suburban highways.

Before Going on a Trip

- Familiarize yourself with local laws and customs in the areas you plan to travel. You are expected to obey their laws, which may include dress standards, photography restrictions, telecommunication restrictions, curfews, etc.
- If you're in an emergency situation abroad, you'll need to know how to contact the police, an ambulance, or the fire department. Not every county uses **911** as its emergency contact number. You can get a list of emergency contact numbers in foreign countries online at https://travel.state.gov/content/dam/students-abroad/pdfs/911_ABROAD.pdf. Write down

the numbers used at your destination countries or save them in your cell phone. Hopefully you won't need to use them, but it's worth knowing them just in case.

- Enroll in the U.S. Department of State's Smart Traveler Enrollment Program (STEP). You can do this online at <http://travel.state.gov/content/passports/english/go/step.html>. It's a free service that allows U.S. citizens and nationals who travel abroad to enroll their trip with the nearest U.S. Embassy or Consulate. When you sign up you will automatically receive the most current information available about the country you will be traveling to. You will also receive updates, including Travel Alerts and Warnings where appropriate. You only need to sign up once. Then you can add and delete trips from your account based on your current travel plans. The STEP will also help the Embassy contact you in an emergency, whether natural disaster, civil unrest, or family emergency. It will also help family and friends get in touch with you in an emergency.
- If you don't enroll in STEP, check the Travel Alerts and Warnings on the U.S. Department of State's website at www.travel.state.gov.
- Go to the U.S. Department of State's Overseas Security Advisory Council (OSAC) website at www.osac.gov for security news and reports for the country(s) you plan to visit. It also has travel alerts and warnings.
- Obtain the phone number and address for the U.S. Embassy or Consulate in the country(s) you plan to visit.
- Plan your wardrobe so it won't offend the locals or draw unwanted attention to yourself. Americans are perceived as wealthy and are targeted for pick pocketing and other crimes. Don't wear expensive-looking jewelry and avoid wearing American team sports shirts or baseball caps that might indicate you are an American.
- Make copies of your passport, airplane ticket, driver license, and credit cards that you take with you. Keep one copy at home and carry a second copy with you but separate from the originals. This will help speed the replacement process if any are lost or stolen.
- Leave all unnecessary identification or credit cards at home. Obtain traveler's checks if needed.
- Provide your family and foreign hosts with ways to contact you in the event of an emergency. Register your trip with the State Department.
- Take any necessary medications with you in their original containers and keep them in your carry-on luggage (not checked baggage) during any flights. Verify you have adequate medical insurance.
- Sanitize your laptop, telephone, and mobile devices to ensure that no sensitive personal data is on them. Backup all information you take and leave it at home. If feasible, use a "clean" laptop, phone, and a new e-mail account. If you can do without the device, don't take it.
- Use up-to-date malware protection, security patches, and firewalls.
- Clean out your voice mail.
- When you access your messages, the pass code may become compromised and others may then retrieve your messages.

Passports

- All passports issued by the U.S. State Department have a small contactless Radio Frequency Identification (RFID) computer chip embedded in the back cover. They are called "Electronic or e-passports." The chip stores the same data that is visually displayed on the photo page of the passport. It also stores a digital photograph of the holder, a unique chip identification number, and a digital signature to protect the stored data from alteration. Unauthorized reading of e-passports is prevented by the addition of a radio-frequency blocking material to their covers.

The passports cannot be read until they are physically opened. Then there are protocols for setting up a secure communication channel and a pair of secret cryptographic keys in the chip to ensure that only authorized RFID readers can read the data on the chip.

- The U.S. State Department now also issues U.S. passport cards that can be used to enter the United States from Canada, Mexico, the Caribbean, and Bermuda at land border crossings or seaports of entry that are less expensive than a passport book. They cannot be used for international travel by air. The card contains a RFID chip to increase speed, efficiency, and security at U.S. land and sea border crossings. However, no personal information is on the chip. It only points to a record stored at secure U.S. government databases. And a protective RFID-blocking sleeve is provided with each card to prevent unauthorized reading or tracking of the card when it is not in use. Make sure you carry the card in the sleeve.

On a Cruise

- Be skeptical. Don't assume you can trust other passengers. Criminals travel too.
- Stay sober. Don't let alcohol impair your judgment. Only drink beverages you have seen prepared. Ask that bottled drinks be served unopened. Don't leave drinks unattended. Someone could slip a drug into one that causes amnesia and sleep.
- Set rules for your children and keep an eye on them. Make sure they don't drink. Report any crew members who serve alcohol to minors.
- Meet fellow passengers in public areas, not cabins.
- Use all locks on your cabin door. Never open it to a stranger.
- When you enter your cabin check the bathroom and closet before closing the door.
- Don't socialize with the crew. Make sure your children know that crew areas are off limits.
- Dress down. Leave expensive jewelry and watches at home. They only make you a target for thieves.
- Lock all valuables in a safe and guard your key card as you would a credit card.
- Don't stand or sit on the ship's railing.
- Never go to any isolated areas of the ship alone, especially in the evening and early morning.
- Know where the members of your party are at all times. Report a missing person immediately.
- Attend the ship safety drills and learn its emergency procedures.
- Bring phone numbers of U.S. Embassies or Consulates in the cities on your itinerary so you can contact them if a problem arises. You can get them online at **www.usembassy.gov**.
- If you are a victim of a crime at sea call the FBI at **(202) 324-3000** from the ship to report the crime. Call the U.S. Embassy or Consulate if you are a victim of a crime on shore. Take photos of the crime scene and any injuries you suffered. Get the names, addresses, and phone numbers of possible witnesses. Take statements. Don't expect the cruise line to take physical evidence. Also notify your family, doctors, lawyers, insurance companies, etc. as appropriate.

Avoiding Trouble in a Foreign Country

- Beware of new acquaintances who probe you for personal information or attempt to get you involved in a possibly compromising situation.
- Avoid civil disturbances. If you come on a demonstration or rally you might be arrested or detained even though you are a bystander.
- Obey local laws. In many countries it is unlawful to speak derogatorily of the government and its leaders or take pictures of train stations, government buildings, military installations, and other public places.

- Avoid actions that are illegal, improper, or indiscreet. Don't do any of the following:
 - Accept offers of sexual companionship
 - Attempt to keep up with your hosts in social drinking
 - Engage in black market activities
 - Sell your possessions
 - Buy illegal drugs or pornography
 - Seek out political or religious dissidents
 - Accept packages or letters for delivery to another place
 - Gossip about character flaws, financial problems, emotional difficulties, or other problems of your fellow Americans or yourself
- Keep a low profile and shun publicity. Don't discuss personal or business information with the local media and be careful what you say to foreigners. They may have been directed to obtain information to hurt you or your business.
- Be aware of your surroundings and alert to the possibility of anyone following you. Report any surveillance to the nearest U.S. Embassy or Consulate.
- Avoid large chain hotels or ones near U.S. Embassies or Consulates, landmarks, religious centers, or places where demonstrations have occurred. Choose a small hotel in a quiet neighborhood.
- Consider the following in choosing a hotel and reserving a room.
 - Has its staff had security and emergency management training in the past year?
 - Does it have an emergency evacuation plan?
 - Are background checks done on all members of its staff?
 - Are there sprinklers in every room?
 - Is security on duty 24/7?
 - Does it have electronic key-card access? Do its elevators require key cards?
 - If rooms are directly over the lobby, reserve a room located between the third and seventh floors. They are within reach of most fire-department ladders.
- Do the following if you are trapped in your hotel by armed assailants:
 - Double-lock your door and barricade it with heavy furniture.
 - Drag a mattress to the center of the room and hunker down under it.
 - Stuff wet towels under the door if there is smoke.
 - Keep quiet so you don't alert attackers to your presence.
 - Avoid windows, a blast outside can be lethal.
- Visit major attractions at less-busy hours.
- Avoid restaurants and clubs frequented by Americans.
- Other safety and security measures for business travel outside the U. S. are contained in a FBI brochure at www.fbi.gov/file-repository/business-travel-brochure.pdf/view.

PROPERTY SECURITY

Protecting Your Home and Property When You Are Away

- Ask the neighbors to watch your home and report any suspicious activities. Make sure they know enough about your life so if they see a stranger around they'll know to report it. For an emergency or a crime in progress they should call **911**. For something suspicious they should call the SDPD's non-emergency number, **(619) 531-2000** or **(858) 484-3154**.
- Invite a neighbor or family member to park a clean vehicle in your driveway. A dirty car that appears to be sitting in the same spot for a long time is a good indicator that you are away.

- Leave your itinerary with a neighbor so you can be contacted in an emergency.
- Lock all doors and windows, even those on the second floor. Use deadbolts, dowels, or locking pins in sliding glass doors and windows to keep them from being pried open.
- Leave window blinds and curtains in their normal daytime positions without exposing any valuable items like a big plasma TV.
- Never announce your vacation plans or whereabouts on Facebook, Twitter, or other social networking sites. In a 2011 survey of 50 convicted burglars in the United Kingdom, 40 said that social media was being used to identify properties with absent owners.
- Wait until you get home to post your vacation blog and photos. Remove geotags with a metadata removal tool if you publish photos on the Internet while you are away. Even better, turn off the geotagging feature on your smartphone.
- Leave lights and a TV or radio on when going out for an evening to make it appear that you are at home.
- Use timers on lights, radios, TVs, etc. to make them go on and off during the day and night to make your home appear occupied.
- Stop mail delivery, or have a neighbor pick it up. This also helps to prevent identity theft.
- Stop newspaper delivery or have a neighbor pick papers up.
- Ask a neighbor to pick up anything left at your door, on your driveway, or elsewhere. And move any empty refuse containers from the curb back into your yard.
- Keep grass watered and cut. Water and trim other landscaping.
- Disconnect your electric garage door opener and padlock the door, preferably on the inside.
- Lock or otherwise secure all pet doors that a person might crawl through.
- Visit your local SDPD Division to request vacation home checks when you'll be out of town. SDPD Division addresses and phone numbers are listed at the end of this paper.
- Set your burglar alarm and notify your alarm company that you will be away. Then if an alarm occurs when you are away the company will not call your home first to verify the alarm. It will notify the police directly. Also provide the alarm company with an up-to-date list of persons to contact about the alarm and the need to secure your home after a burglary.
- If you have a house or pet sitter, familiarize that person with your home's security systems and procedures and stress the importance of following them.

You should also consider authorizing the SDPD to act as you agent and enter your property for purposes of enforcing laws against any person(s) found on the property without your consent or lawful purpose. To do this you should talk to the CRO in your area about filing a Letter of Agency. The form for this Letter must be filled out on the SDPD website in the following steps and filed by clicking on Email Form on the bottom left. You can skip the first step if you know what SDPD Division covers your home.

1. Go to **www.sandiego.gov/police/pdf/2013policecitywidemap.pdf** to find out what SDPD Division covers the neighborhood in which your property is located.
2. Go to the Forms page on the SDPD website at **www.sandiego.gov/police/forms/forms** and click on Trespass Authorization/Letter of Agency Form.
3. Click RESET FORM to get the start and expiration dates. The Letter must be renewed every 12 months.
4. Use the drop down menu to enter the Police Division.
5. Fill in the blue blanks on the form.

After a Letter of Agency has been filed, you can post NO TRESPASSING signs stating that a Letter has been filed with the SDPD. The sign would have the address of the property, the name and phone number of the property owner or manager, and the non-emergency SDPD phone number to report suspicious activities. That number is **(619) 531-2000** or **(858) 484-3154**. The signs should be at least 18 by 24 inches in size, have a font visible from the nearest public street, not be accessible to vandals, and be posted on the entrances and spaced evenly on the boundaries of the property. A sample sign is available by clicking on View a Sample Sign on the Forms page of the SDPD website at www.sandiego.gov/police/forms/forms.

Credit Freeze and Use of Credit Cards

- Take only essential credit cards. Leave debit cards at home in a secure place. Consider carrying two credit cards, keeping one in a safe place in case the other one is lost or stolen.
- Consider placing a security freeze, sometime called credit freeze, on your credit files with the three CCRBs. A security freeze means that your file cannot be shared with potential creditors. It will generally stop all access to your credit files, but may not stop misuse of your existing accounts or other types of identity theft. It can help prevent identity theft because most businesses will not open credit accounts without first checking a consumer's credit history. If your credit files are frozen, even someone who has your name and SSN would probably not be able to get credit in your name. For California residents a security freeze is free to identity theft victims who have a police report of the theft. It is also free to residents age 65 and older. If you are not an identity theft victim and you are under age 65, it will cost you \$10 to place a freeze with each of the three CCRBs. That is a total of \$30 to freeze your files. You should keep the freezes on when you return for identity theft protection. You can always lift the freeze if you want someone to see your credit file, e.g., if you are applying for credit, insurance, or employment. For more information about security freezes see the answers to frequently-asked questions published by the California Attorney General on a page entitled *How to "Freeze" Your Credit Files* at www.oag.ca.gov/idtheft/facts/freeze-your-credit. You can place freezes on your credit reports by contacting Equifax at **(800) 349-9960**, Experian at **(888) 397-3742**, and TransUnion at **(888) 909-8872**. Or you can request a freeze online at these websites: www.freeze.equifax.com, www.experian.com/freeze/center.html, and www.transunion.com/credit-freeze/place-credit-freeze. You'll need to supply your name, address, date of birth, SSN, and other personal information. After receiving your freeze request by phone, each CCRB will send you a confirmation letter containing a unique PIN or password to use if you choose to lift the freeze. If you request a freeze online, you can download your PIN.
- Call your credit card companies using the customer service number on the back of the card to alert them about when, where, and how long you will be away. This will enable their fraud departments to stop charges if your card is used elsewhere, and reduces the risk that charges made where you are going to be will not be accepted. Or you can do this online if your card issuer has a "travel notification" or similar tab that you can use when you log onto your account.
- Credit cards with embedded microchips are extremely difficult to counterfeit or copy. They are now standard in Canada, Mexico, Europe, and many other countries, and will be mandatory in the United States by October 2015. In the meantime cards without these chips may be rejected in many places. If your card issuer offers micro-chipped cards, you should get one before travelling to these countries.
- Consider using Virtual Account Numbers (VANs) for your credit cards. They offer one-time use and are disposable. Some credit card companies offer them. Here's how they work. Log onto your credit card account and generate a random account number. Enter it on the merchant's

bill instead of your real account number. This VAN will only be valid for the time it takes the merchant to process your transaction. Your credit card company will recognize it and charge the amount to your account. If a hacker breaks into the merchant's computer and steals your VAN, it will be useless. Note that VANs cannot be used for purchases that require you to show your credit card at time of pick-up (e.g., movie tickets, etc.), because the account numbers won't match. VANs make it virtually impossible for anyone to steal your real account number from a merchant. A variant on a VAN is a temporary card number that has a spending limit, expiration date, and security code that you can use for multiple online transactions.

- Inform your credit card companies when you return and review transactions for the period you were gone. Continue to monitor your personal financial account transactions for unauthorized or unapproved use.
- Some credit cards now have embedded RFID chips that are designed to be read by secure card readers at distances of less than 4 inches when properly oriented for "contactless payments." Thus, RFID readers that are available to the general public and can operate at ranges up to 25 feet and are essentially useless in stealing the information on your card. And even if that information is "hi-jacked," the cards are said to have security features that make it difficult or impossible to make a fraudulent transaction. Furthermore, the information on the chip is not the same as that on the magnetic stripe, and it cannot be used to create a functioning counterfeit version of the card. If you are concerned about unauthorized reading or tracking of the card when it is not in use, you can buy a protective RFID-blocking sleeve for the card. Make sure you carry the card in the sleeve. And if you have a card with a RFID chip and don't want to risk having the information on it stolen and used in any fraudulent activity, ask your card company for a new card without a chip. Or better, request a new card with new Europay, MasterCard and Visa (EMV) technology. These cards have a secure microchip that is designed to make them very difficult and expensive to counterfeit. Also, the chip stores encrypted data about the cardholder account, as well as a "cryptogram" that allows banks to tell whether a card or transaction has been modified in any way.

At a Hotel or Motel

- Use all available locks on the doors and windows.
- Make sure the door is securely locked when you leave your room.
- Unpack and place your belongings in the closet and dresser. Arrange things so you can easily tell if something is missing. Keep a list of all things you brought from home.
- Lock your suitcases so they cannot be used to carry things out. Consider hiding electric appliances and other valuable items in your suitcase.
- Don't leave cash, checks, credit cards, jewelry, vehicle keys, etc. in the room. Take them with you or lock them in the hotel safe.
- Report any lost or stolen items to the hotel management as well as to the police.
- Don't use hotel computers for anything that requires passwords or personal information. You never know if any identity-stealing software is installed.
- Never give out any personal information to someone who calls and says he or she is at the front desk and needs the information. Ignore the request and go to the desk yourself to see if any information is needed.
- If you have to leave your passport at the desk ask for a receipt and be sure to retrieve it when you check out.

On a Train

- Don't leave any valuables unattended. Thefts from sleeping compartments are common.

When Out and About

- Carry only a driver license, a minimum amount of cash (some small bills for tipping), traveler's checks, a credit card with a low charge limit, and insurance cards. Don't carry blank checks or a checkbook. Don't carry anything with PINs, account numbers, or passwords written on it. And don't carry a debit card.
- Know your destination's exchange rate. Never exchange money on the black market. Always deal with a reputable currency exchange or you risk getting counterfeit currency.
- Check that your prescription drugs are legal at your destination.
- Carry prescription drugs in their original containers.
- Don't carry your Social Security card or anything with your SSN on it. Persons with Medicare cards should carry photocopies of the cards with the last four digits of their SSN removed. Keep the card in a safe place at home and bring it if needed for a doctor appointment.
- Make a list of all the cards you carry. Include all account numbers and phone numbers to call to report a lost or stolen card. Also make photocopies of both sides of all the cards. (If you carry a library card, make a copy of it too.) Keep the list and copies in a safe place at home. Also bring copies to put in your hotel safe along with copies of your passport, tickets, traveler's check numbers, an extra credit card, and other important papers.
- Don't carry personal information of your family members.
- It's better to leave anything you don't need at home.
- Avoid carrying a purse if possible. Wear a money pouch instead.
- Carry a purse with a shoulder strap if you must. Keep the strap over your shoulder, the flap next to your body, and your hand on the strap. Hang the purse diagonally across your body.
- When wearing a coat and carrying a purse, conceal the strap and purse under the coat.
- Keep a tight grip on your purse. Don't let it hang loose or leave it on a counter in a store.
- Carry your wallet, keys, passport, and other valuables in an inside or front pants pocket, a fanny pack, hidden pouch, or other safe place. Don't carry a wallet in a back pocket.
- If you have an empty pocket, carry a spare wallet you can give to a robber. Put a few dollars, an expired credit card, and an old hotel key card in it.
- Be wary of street vendors and innocent-looking youngsters. While one has your attention, another might be picking your pocket.
- Avoid crowds and long lines. These places harbor pickpockets and other criminals.
- Never put your purse or wallet on a counter while shopping.
- Some credit cards now have embedded RFID chips that are designed to be read by secure card readers at distances of less than 4 inches when properly oriented for "contactless payments." Thus, RFID readers that are available to the general public and can operate at ranges up to 25 feet and are essentially useless in stealing the information on your card. And even if that information is "hi-jacked," the cards are said to have security features that make it difficult or impossible to make a fraudulent transaction. Furthermore, the information on the chip is not the same as that on the magnetic stripe, and it cannot be used to create a functioning counterfeit version of the card. If you are concerned about unauthorized reading or tracking of the card when it is not in use, you can buy a protective RFID-blocking sleeve for the card. Make sure you carry the card in the sleeve. And if you have a card with a RFID chip and don't want to

risk having the information on it stolen and used in any fraudulent activity, ask your card company for a new card without a chip.

What to Do If Your Purse or Wallet Is Lost or Stolen

- File a police report in the jurisdiction where your wallet was lost or stolen. Also file one in the jurisdiction where you live. Get a copy of the report. You may need to send copies elsewhere.
- Report the loss to one of the three Consumer Credit Reporting Bureaus (CCRBs). Their phone numbers are: **(800) 525-6285** for Equifax, **(888) 397-3742** for Experian, and **(800) 680-7289** for TransUnion. And request that an initial fraud alert be placed on your credit files. The CCRB you call is required to notify the other two. A fraud alert will tell creditors to follow certain procedures before they open a new account in your name or make changes to your existing account. In doing this you will be entitled to free copies of your credit report from each CCRB. Order them a few weeks after your loss and review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Fraud alerts are good for 90 days and can be renewed. They are free. This alert may prevent someone from opening a new account in your name but it will not prevent misuse of your existing accounts.
- Alert your banks of the loss and request new account numbers, checks, ATM cards, and PINs. Also provide new passwords and stop payment on any missing checks.
- Contact all your creditors by phone and in writing to inform them of the loss.
- Call your credit card companies and request account number changes. Don't ask to cancel or close your accounts; that can hurt your credit score, especially if you have outstanding balances. Say you want a new numbers issued so your old numbers will not show up as being "cancelled by consumer" on your credit reports.
- Call the security or fraud departments of each company you have a charge account with to close any accounts that have been tampered with or established fraudulently. Follow up the request in writing and ask for written verification that the accounts have been closed and any fraudulent debts discharged. Keep copies of all documents and records of all conversations about the loss. If you still want a charge account, request a new number.
- If your Social Security card or any other card with your SSN on it was in your purse or wallet, contact your local police and the IRS as suggested above. Also contact the Social Security Administration (SSA) at **(800) 772-1213** to request a replacement card or go to **www.ssa.gov/ssnumber** to apply for one online.
- If your Medicare card or any other card with your Medicare number on it was in your purse or wallet, contact your local police and the IRS as suggested above. Also contact the SSA at **(800) 772-1213** to request a replacement card. Or to obtain one online you need to first create a My Social Security account as explained at **<https://faq.ssa.gov/ics/support/kbanswer.asp?deptID=34019&task=knowledge&questionID=3708>**.
- If your driver license was lost, contact the California DMV Fraud Hotline at **(866) 658-5758** to report the loss, request a replacement license, ask that a stolen/lost warning be placed in your file, and check that another license has not been issued in your name.
- If your library card was lost, contact the library immediately. Otherwise you could be held financially responsible for any material borrowed after the loss.
- If you lose your automobile, homeowners, or health insurance cards, notify the companies and request replacements.
- If your passport was lost or stolen in the United States, report it to the U. S. Department of State by calling **(877) 487-2778**. Operators are available from 8 a.m. to 10 p.m. ET, weekdays

excluding Federal holidays. Or you complete, sign, and submit Form DS-64, Statement Regarding a Lost or Stolen Passport, to the U. S. Department of State, Passport Services, Consular Lost/Stolen Passport Section, 1111 19th St. NW, Ste. 500, Washington DC 20036. If it was lost or stolen overseas contact the nearest U. S. Embassy or Consulate.

- To replace a lost or stolen passport in the United States submit Forms DS-11, Application for a U. S. Passport and DS-64 in person at a Passport Agency or Acceptance Facility. If you are overseas, go to the nearest U. S. Embassy or Consulate if you are overseas to replace it.

Using Wi-Fi, Laptops, and Mobile Devices in Public Places

The following tips are provided by the U.S. Department of Homeland Security's Transportation Security Administration. Also see the SDPD paper on cybersecurity at www.sandiego.gov/sites/default/files/cybersecurity.pdf for steps to take to reduce the risks of using Wi-Fi, laptops, and mobile devices in public places.

- Be aware that using Wi-Fi in coffee shops, libraries, airports, hotels, universities, and other public places poses major security risks. While convenient, they're often not secure. You're sharing the network with strangers, and some of them may be interested in your personal information. If the hotspot doesn't require a password, it's not secure.
- Also be aware that unsecure laptops and mobile devices like smartphones make it easy for a hacker to intercept information to and from the web, including passwords and credit- or debit-card numbers. They are also vulnerable to virus and spyware infections, and to having their contents stolen or destroyed.
- Install the latest operating system in your mobile devices and download all security software updates into your laptops. This will protect you from current viruses, worms, spyware, Trojan horses, spam, and other dangerous malware.
- Before you connect to any public Wi-Fi in a hotel, airport, train/bus station, café, or other place you should confirm the name of the network and its login procedures with an appropriate person to ensure that the network is legitimate.
- Don't use public Wi-Fi to perform sensitive transactions such as banking and online purchases.
- Always check your surroundings in public places to ensure that no one can view sensitive information on your screen or the keys you use to enter information.
- Never leave your mobile devices, including any USB/external storage devices, unattended in a public place. And if you plan to leave them in your hotel room, make sure they are appropriately secured.
- Make sure you take your mobile devices, including any USB/external storage devices, with you when you leave a public place.
- Turn off a Bluetooth-enabled device when it is not in use to prevent someone from connecting to your device and gaining access to your sensitive information.
- Never connect your mobile devices to any public charging station to prevent malicious software from being installed and/or access to your sensitive information.

Preventing Vehicle Break-Ins

The following tips help prevent vehicle break-ins, which could lead to theft of the vehicle itself or of things items in it.

- Park in an open, well-lighted, and populated area near your destination, preferably one in view of a security camera. Avoid parking near trucks, vans, camper shells, dumpsters, and other objects that obstruct visibility and provide hiding places. Also avoid parking near people loitering or sitting in vehicles.
- Never leave anything in plain sight, not even empty bags or boxes. Conceal all navigation aids, cellular phones, audio systems, sunglasses, etc. inside your vehicle. Put cameras, packages, sports equipment, firearms, hand tools, and other valuables in the trunk before you park, never after you park because thieves may be watching. And take anything you can't afford to lose with you, e.g., a wallet, purse, or laptop computer. Thieves usually don't break into vehicles unless they plan to steal what's visible inside.
- Park in lots or garages where you don't have to leave your keys.
- Turn off your engine, roll up all windows, lock all doors, and take your keys with you even if you are making a quick stop at a store or gas station. Also make sure the trunk and hood are locked.
- Don't leave your vehicle in an unattended public lot for an extended period time.
- If your vehicle has an alarm system that will sound when someone attempts to break in, move, tilt, or start your vehicle, always activate it when leaving the vehicle.
- Check your vehicle if you hear the alarm sound. But don't try to stop a person attempting to break in. Get a good description of the person and call the police.
- If you lock your vehicle with a Remote Keyless Entry (RKE) fob, make sure that all the doors are locked before leaving your vehicle, especially in public parking lots. There has been an increased use of jammers to prevent the RKE signal from activating the door locks.

Preventing Thefts of Parked Vehicles

The following tips are in addition to the ones listed above for preventing vehicle break-ins.

- Conceal maps or travel brochures that might indicate you are a tourist.
- Turn your wheels sharply toward the curb when parking on a street.
- Use anti-theft devices that can be attached to the steering wheel or column, or brake pedal.
- Don't hide a spare key on your vehicle.

Preventing Thefts from Vehicles

The following tips are in addition to the ones listed above for preventing vehicle break-ins.

- When shopping, ask the store to hold all your purchases until you are finished there so you can carry everything to your vehicle in one trip. If you need to make more than one trip, put your purchases in the trunk and move your vehicle to a different area of the parking lot after each trip.
- Make sure that any valuables that were locked in the glove box or trunk were not taken or tampered with when you return to your vehicle. Thieves are able to get into some vehicles without leaving any visible signs of a break-in.
- Take the face of your CD player with you if it is removable.
- Lock truck-bed toolboxes.
- Make several slices through your license plate registration sticker after it has been placed on the plate. If the sticker is stolen you can get a replacement from your local Department of Motor Vehicles (DMV) office.

- When pumping gas and no one else is in your vehicle, roll up all the windows, lock the doors, and take your keys with you so you don't lock yourself out of the vehicle. This will prevent someone from taking anything you may have left in the vehicle, e.g., a purse on the front seat, while you are not looking.

SDPD DIVISIONS

Central	2501 Imperial Ave. SD 92102	(619) 744-9500
Eastern	9225 Aero Dr. SD 92123	(858) 495-7900
Mid-City	4310 Landis St. SD 92105	(619) 516-3000
Northeastern	13396 Salmon River Rd. SD 92129	(858) 538-8000
Northern	4275 Eastgate Mall SD 92037	(858) 552-1700
Northwestern	12592 El Camino Real SD 92130	(858) 523-7000
Southeastern	7222 Skyline Dr. SD 92114	(619) 527-3500
Southern	1120 27th St. SD 92154	(619) 424-0400
Western	5215 Gaines St. SD 92110	(619) 692-4800
