DECEMBER HOLIDAY SAFETY AND SECURITY TIPS
SDPD Crime Prevention
April 13, 2017

CONTENTS

AT HOME
AWAY FROM HOME
WHEN DRIVING AND PARKING
WHEN SHOPPING
CHILDREN
ONLINE

Holidays are special times to be shared with family and friends. Protect yourself and loved ones by following these safety tips. For more tips, see the SDPD papers on Home Security, Personal Safety and Security, Cybersecurity, Fraud and Identity Theft Prevention, and Vehicle Security on its website at **www.sandiego.gov/police/services/prevention/tips**.

AT HOME

- Don't put large displays of holiday gifts in view of your windows or doors.
- Immediately after the holidays, mark new gifts with your California Driver License or ID number.
- Don't advertise what you got for Christmas by putting the boxes out on trash day. Break the boxes down or take them to the dump yourself.
- Don’t open your door at the sound or a knock or bell. Know who’s at your door before opening it. Install a wide-angle peephole in your front door so you can look out without being seen yourself.
- If you don’t want to answer the door and don’t want the person there to think that no one is home, say something like “We can’t come to the door now,” or “We don’t open the door to strangers.”
- Don’t open the door to a delivery person unless you are expecting a package. Ask for the person’s name and the name and phone number of the company. Call it to confirm the visit. Keep the door closed and locked in the meantime.

AWAY FROM HOME

- Lock all doors and windows, even if you will only be gone for a short time. 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.
- 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 neighbor pick it up. (This also helps to prevent identity theft.)

- Stop newspaper delivery or have neighbor pick them up. Also have neighbor pick up anything left at your door, on your driveway, or elsewhere.
- Arrange to have packages delivered to a neighbor will be home during the day.
- Keep grass watered and cut. Water and trim other landscaping.
- Ask the neighbors to watch your home and report any suspicious activities.
- Invite a neighbor or family member of park a vehicle in your driveway.
- Leave your itinerary with a neighbor so you can be contacted in an emergency.
- 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.
- Install a good side-yard gate and keep it locked at all times. Side and back entries are the most common access points for burglars.
- Visit your local SDPD Area Station to request home checks while you are away.
- 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.

WHEN DRIVING AND PARKING

- In a lot, park as close a possible to the store entrances, preferably 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 who are loitering or sitting in vehicles. Check that no one is near your vehicle before you get out.
- In a garage, park where you don't have to use stairs or elevators.
- If you use valet parking, don't leave your home keys on a chain with your vehicle keys. Also, don't leave your garage door opener where it is easily accessible. Keep your vehicle registration, proof of insurance, and any other papers with your home address on them where they are not likely to be found.
- At night, park in t well-lighted area.
- Remember where you parked so you can return directly to your vehicle.
- Lock your vehicle, and make sure the windows are closed. 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. Thieves may be watching. And take anything you can't afford to lose with you, e.g., a wallet, purse, or laptop computer. Thieves don't break into vehicles unless they plan to steal them or take what's visible inside.
- Never leave children alone in your vehicle.
- Be alert and walk away purposefully. Avoid walking near strangers loitering or sitting in vehicles.
- Have someone escort you to your vehicle if you are concerned about safety. Or wait until other people you can walk near.
- Don't approach your vehicle alone if there a suspicious people nearby.
- Don't overload yourself with packages. Use a cart or shop with a partner who can help carry packages. There is safety in numbers.
- 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. The key can be used as a defensive weapon if necessary.
- 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 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.

WHEN SHOPPING

- Shop during the day. If you must shop in the evening, shop with a friend.
- Dress casually and comfortable. Don't wear flashy or expensive jewelry.
- Carry only the charge cards you will need. Don't carry large sums of cash. When charging an item, make sure you get your card back. Use a credit card when possible.
- Bring home all transaction receipts. Never or throw them in public trashcans. Dispose of them at home after matching them against your monthly statements. Look for charges you didn't make. Notify your card companies or financial institutions immediately of any you find.
- Report all lost or stolen cards immediately and request cards with new numbers. Keep a record of all credit card numbers and the customer-service phone numbers you should call. Put it in a safe place.
- Carry purses next to your body with the purse flap against you and locked or zipped. Use a strap that goes diagonally across your body. Carry wallets in front or inside pockets. Purses and wallets are prime targets of thieves.
- Don't get distracted and leave your purse or wallet on a transaction counter or in a shopping cart.
- Don't hesitate to notify store security if you see any suspicious people or activities.
- If you have to wait for a ride, wait in a busy, well-lighted place.
- If you are a victim of a crime, call **911** to report it police immediately.

CHILDREN

- If possible, leave them at home with a trusted sitter.
- Have them stay with you at all times. Tell them not to wander off, leave the store, or hide. Don't get distracted by the sights, sounds, and crowds.
- Accompany them to restrooms.
- Never leave them at a video arcade, food court, toy store, or play area as a convenient "babysitter." Personnel in those areas are not there to watch children.
- Never leave them alone in your vehicle.
- If you allow an older child to go off without you, have him or her go with a friend and set a time for them to return or meet you at a designated place. Also, agree on what to do if plans change.
- Tell them to go to the nearest uniformed security guard or salesperson with a nametag and ask for help if they become separated. Show these people to your children when you enter the store or walk through a mall.
- Make IDs for them to carry in their pockets.
- Report a missing child immediately if you get separated. Carry a recent color photo and describe the clothes he or she is wearing. Contact store or mall security first. Call **911** if the child is not found soon.

ONLINE

The following tips are from a scam alert entitled *Don't Let Scammers Take Away Your Holiday Cheer* dated November 23, 2016 on the Federal Trade Commission (FTC) website at **www.consumer.ftc.gov/blog/dont-let-scammers-take-away-your-holiday-cheer**. It recommends the following ways to avoid giving your hard-earned money to a scammer during the holiday season.

- Know how NOT to pay. If someone asks you to pay with an iTunes or Amazon gift card or tells you to wire money through services like Western Union or MoneyGram, don't do it. Scammers ask you to pay in ways that let them get the money fast and make it nearly impossible for you to get it back. If you're doing any holiday shopping online, know that credit cards have a lot of fraud protection built in.
- Spot imposters. Imposters pretend to be someone you trust to convince you to send money or personal information. They might send phishing e-mails that seem to be from your bank asking you to "verify" your credit card or checking account number. Don't do it. Learn more about spotting imposter scams at **www.consumer.ftc.gov/features/feature-0037-imposter-scams**.
- Make sure your money goes to real charities. The holidays are a good time to share with people in need. Unfortunately, sometimes scammers try to take advantage of your good will. And even when you're dealing with legitimate charities, it's still important to check it out. Go to **www.consumer.ftc.gov/articles/0074-giving-charity f**or precautions to take to make sure your donation benefits the people and organizations you want to help.

- Sign up to get free FTC scam alerts by e-mail by clicking on the box at **www.consumer.ftc.gov/scam-alerts**.

Online shopping has become a popular way to purchase items without the hassles of traffic and crowds. However, because the Internet has unique risks it is important to take steps to protect yourself when shopping online. The U.S. Computer Emergency Readiness Team (US-CERT) Security Tip ST07-001 entitled S*hopping Safely Online*, last revised on October 1, 2016 at **www.us-cert.gov/ncas/tips/ST07-001** describes how attackers target online shoppers and how you can protect yourself.

Attackers can take advantage of online shoppers in the following ways.

- Creating fraudulent sites and e-mail messages. They may also misrepresent themselves as charities, especially during the holiday season. They create these malicious sites and e-mail messages to get you to supply personal and financial information.
- Intercepting insecure transactions. If a vendor does not use encryption, an attacker may be able to intercept your information as it is transmitted.
- Targeting vulnerable computers. If you don't protect your computer from viruses or other malicious code, an attacker may be able to gain access to your computer and all of the information on it. It is also important for vendors to protect their computers to prevent attackers from accessing customer databases.

Here are some ways to protect yourself and minimize your risks.

- Do business with reputable vendors. Because some attackers try to trick you by creating malicious websites that appear to be legitimate, you should check their legitimacy before supplying any information. See the US-CERT Security Tip ST05-010 entitled *Understanding Web Site Certificates*, last revised October 1, 2016, at **www.us-cert.gov/ncas/tips/ST05-010** for ways to check a site certificate. Also, locate and note phone numbers and physical addresses of vendors in case there is a problem with your transaction or bill.
- Make sure your information is being encrypted. Many sites use Secure Sockets Layer (SSL) to encrypt information. Indications that your information will be encrypted include a URL that begins with **https** instead of **http** and a padlock icon. If the padlock is closed, the information is encrypted. The location of the icon varies by browser. Some attackers try to trick users by adding a fake padlock icon, so make sure that the icon is in the appropriate location for your browser.
- Be wary of e-mails requesting information. Attackers may send e-mails that ask you to confirm a purchase or provide account information. Legitimate businesses will not do this. See the US-CERT Security Tip ST04-014 entitled *Avoiding Social Engineering and Phishing Attacks*, last revised October 1, 2016, at **www.us-cert.gov/ncas/tips/ST04-014** for ways to avoid being a victim of these tactics.
- Use a credit card. There are laws to limit your liability for fraudulent credit card charges, but you may not have the same level of protection for your debit cards. Additionally, because a debit card draws money directly from your bank account, unauthorized charges could leave you with insufficient funds to pay other bills. You can minimize potential damage by using a single, low-limit credit card to making all of your online purchases. Also use a credit card when using a payment gateway such as PayPal, Google Wallet, or Apple Pay.
- Check your shopping app settings. Look for apps that tell you what they do with your data and how they keep it secure. Keep in mind that there is no legal limit on your liability with money stored in a shopping app or on a gift card. Unless otherwise stated under the terms of service, you are responsible for all charges made through your shopping app. See the FTC Consumer Information page entitled *Apps to Help You Shop in Stores* that provides answers to the following questions: What Can Shopping Apps Do? What if I Discover a Billing Error? And What Personal Information Do Shopping Apps Collect? It's online at **www.consumer.ftc.gov/articles/0515-apps-help-you-shop-stores**.
- Check your statements. Keep a record of your purchases and copies of confirmation pages, and compare them to your bank statements. If there is a discrepancy, report it immediately. See the US-CERT Security Tip ST05-019 entitled *Preventing and Responding to Identity Theft*, last revised October 1, 2016, at **www.us-cert.gov/ncas/tips/ST05-019** for more information on this and other ways to avoid being a victim.
- Check privacy policies. Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used. See US-CERT Security Tip ST04-013 entitled *Protecting Your Privacy* at **www.us-cert.gov/ncas/tips/ST04-013** for additional steps can you take to protect your privacy.

US-CERT reminds Internet users to be aware of the following other scams at holiday times.

- Unsolicited shipping notifications that may actually be scams to solicit personal information
- E-mail notification of e-cards that appear to be from a legitimate card company but will download malware into your computer when you click on the link to see the card
- Requests for charitable contributions that may be phishing scams or solicitations from sources that are not real charities
- False advertisements for holiday accommodations or timeshares.