HOME SECURITY TIPS
SDPD Crime Prevention
July 11, 2017

CONTENTS

CONTROLLING ACCESS
- Physical Protection
- Deterrent Measures
- Burglar Alarms
- Cameras in Homes
- Cameras in Multi-Family Buildings
- Procedures
- What Burglars Say

SMART HOME SYSTEMS
PROVIDING VISIBILITY
MAINTAINING YOUR PROPERTY
PROTECTING YOUR HOME AND PROPERTY WHEN YOU ARE AWAY
HELPING TO PREVENT RESIDENTIAL BURGLARIES IN YOUR NEIGHBORHOOD
MAKING SURE THE POLICE CAN FIND YOUR HOME
IDENTIFYING YOUR PROPERTY
PREVENTING EMPLOYEE AND CONTRACTOR THEFT

Burglary is mostly a crime of opportunity that capitalizes on the carelessness and neglect of the homeowner or renter. This paper contains tips on preventing home burglaries, vandalism, and other property crimes by controlling access, providing visibility, and maintaining your property. It also contains tips on protecting your home and property when you are away, helping to prevent residential burglaries in your neighborhood, and preventing employee theft. And if you do become a victim, it includes tips on making sure the police can find your home, and on identifying your property. These tips can significantly enhance the security of your home and property.

Additional tips on personal safety and security, vehicle security, travel safety and security, senior safety and security, preventing crimes against businesses, preventing fraud and identity theft, reporting crime and suspicious activities, reporting suspicious activities for terrorism prevention, reporting disorder and other problems, obtaining crime information, dealing with homeless people, and starting a Neighborhood Watch program can be found in the Crime Prevention and Education section of the SDPD website at **www.sandiego.gov/police**.

CONTROLLING ACCESS

The following tips suggest how access to your home, apartment, or condo can be controlled by physical protection, deterrent measures, and various procedures.

Physical Protection

- Install single cylinder dead-bolt locks on all doors. Bolts should have a minimum throw of 1 inch. Strike plates should have screws that are at least 3 inches long. Doors should be solid hardwood or metal clad. Hinges should be located on the inside or have non-removable pins. Special locks are need on double and Dutch doors. French doors that burglars easily break through should be made with a burglar-resistant material that meets Underwriters Laboratories (UL) 972 standards.

- Mount a steel reinforcing device on the lock side of all exterior wood door frames. It will prevent a burglar from kicking in the door. To be effective it should extend well above and below the strike plate.
- Install locking devices on all sliding glass doors and windows.
- Install good locks all doors that lead outside through garages or storage areas.
- If you have a pet door, it should be the smallest your pet can get through. If you have a large pet and a person can squeeze through the door, you'll have to rely on locked side-yard gates to keep a burglar out.
- Don't rely on chain locks for security. They're only good for privacy.
- Re-key or change all locks when moving into a new home. Make sure the locksmith is licensed by the California Bureau of Security and Investigative Services. You can verify a license at **www.bsis.ca.gov/forms_pubs/online_services/verify_license.shtml** for companies and company employees. You should also see if the locksmith is a member of the Associated Locksmiths of America (ALOA). It is an association of certified locksmiths and security experts who represent the highest level of professionalism, experience, and reliability in the industry. Go its website at **www.aloa.org**, click on Find a Locksmith, and enter a ZIP and a search radius.
- Install locks on gates, garages, sheds, etc.
- Go to a locksmith or hardware store for advice on locks.
- All locks should be resistant to "bumping"
- Screen security doors should have the following features so they cannot be broken through or pried open:
  - Four-sided, stainless-steel frame
  - Frame secured to home
  - Steel mesh that cannot be cut with a knife
  - Mesh secured to frame to resist dynamic impacts
  - Rust and corrosion resistant
  - Passed Australian Standards (AS) knife shear, dynamic impact, jimmy, and salt spray tests
  - Multi-point locking
  - Deadbolt lock with key that can only be duplicated by manufacturer
- Use a burglar-resistant material that meets UL 972 standards in all windows and doors that a burglar might try to break through. These materials look like standard glass but will not shatter easily, even after repeated blows. The following materials can be used:
  - *Laminated glass* is made with a vinyl or plastic inter-layer sandwiched between two layers of glass. This type of glass adds additional strength to your windows. To gain entry a burglar would have to strike the glass repeatedly in the same spot in order to make a small opening. Most burglars are reluctant to create this type of noise for fear of being detected.
  - *Tempered or safety glass* is made by placing a piece of standard glass in an oven, bringing it almost to the melting point, and then chilling it rapidly. This causes a skin to form around the glass. Fully tempered glass is four to five time stronger than standard glass.
  - *Wired glass* adds the benefit of a visible deterrent. Extra effort will be needed to break the glass and then cut through the wire located within the glass in order to gain entry.
  - *Plastic acrylics* are more than ten times stronger than glass of the same thickness and are commonly called Plexiglas.
  - *Polycarbonate* sheets are superior to acrylics and are advertised as 250 times more impact resistant than standard glass, and 20 more times than other transparent plastic.

  Glass with a security film attached to the inside can also be burglar-resistant. It requires repeated blows to break through, which take time and make noise. A burglar faced with this task might give up and go away or look for another way or place to break in.
- Consider installing security bars on side, rear, or other windows that a burglar might break to enter your home. Bars must comply with Fire Code requirements for inside release to permit an occupant to escape in the event of a fire.
- Keep valuables in a bank safe deposit box or a home safe that is hidden and bolted down.
- Fence in the yard.
- 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. The gates and adjacent fencing should be at least 6 feet high. The best way to lock a gate is with a hidden-shackle or shielded padlock that conceals both the shackle and the hasp so they cannot be cut with a bolt cutter. Wrought-iron gates that are opened on the inside by a lever arm or knob should have shields on the gates and the adjacent fencing to prevent a person from reaching in to open them. These shields can be

solid plastic or metal, or open metal mesh. Gates with lever-arm locks should also have a cylindrical shield around the inside arm that prevents a person from opening the gate by inserting anything through, over, or under the gate that can be used to rotate the arm, e.g., a thin wire with a hook at one end. Gates with locks that have beveled latches should also have a latch guard to prevent a person from inserting a thin piece of metal or anything else between the frame and the gate to push in the latch. The guard should be centered on the latch and extend at least 12 inches above and below it. A deadbolt lock would not have this problem, nor would a gate with a padlock.

- Plant bushes with thorns or prickly leaves near windows and along fences.
- Trim trees so that limbs don't provide access to roofs, second stories, etc.
- Call the SDPD Community Relations Officer (CRO) in your neighborhood to arrange for a free home security survey. SDPD Division Station addresses and phone numbers are listed at the end of this paper.

Deterrent Measures

- Put alarm company stickers on entry doors and windows.
- Consider having a dog that can scare a stranger away by either barking or looking fierce. Keep an outside dog in a fenced area and have a good lock on the gate.
- Use fencing, gates, landscaping, pavement treatment, signs, etc. to define clear boundaries between your property and adjoining properties.

Burglar Alarms

Alarm systems usually include one or more of the following components: photocell or magnetic contacts on doors and windows, heat or motion detectors in interior spaces, glass break detectors, keypads with a means of checking the status of the system, garage door monitor, and audible alarms. If you don't have sensors on your windows, install motion detectors that will detect break-ins and trigger an alarm. All equipment should be UL certified. Multiple sensors are preferred because they reduce false alarms, which are wasteful of police resources and lead to fines and permit revocation. The system should also have a fail-safe battery backup. If your system is monitored, the monitoring station should be open 24/7 and have backup power. The company's customer service department should also be open 24/7.

Do before choosing an alarm company:

- Read the brochure *Consumer Guide to Alarm Companies*. It is published by the California Bureau of Security and Investigative Services (BSIS) and is available online at **www.bsis.ca.gov/forms_pubs/alarmco.pdf**. Or call **(800) 952-5210** to have a copy mailed to you.
- Get alarm company references from your insurance agent, family members, friends, or neighbors. Get at least three estimates in writing. The SDPD does not prefer or recommend companies, brands, or types of security systems.
- Obtain estimates for similar systems that provide the same level of protection. Be sure that the initial installation change and monthly monitoring fees are included.
- Make sure the alarm company has a City Business Tax Certificate and is licensed by the California BSIS. You can verify the latter by calling **(800) 952-5210** or going online at **www.bsis.ca.gov/forms_pubs/online_services/verify_license.shtml**.
- See if the company is a member of the Electronic Security Association (ESA). Go it its website at **www.alarm.org** and under Consumers, click on Looking for an Alarm Dealer and then click on California to get a list of member companies. The ESA has adopted a strict code of ethics that addresses consumer concerns and provides a process for consumer complaints. You can read this code in its website as well as helpful tips for choosing an alarm company.
- Call the Better Business Bureau of San Diego County at **(858) 496-2131** to check on any unsolicited offers, especially those from a door-to-door salesperson. Or visit its website at **www.sandiego.bbb.org** to see whether the business is accredited. You can also check its rating, reason for the rating, and the number of closed complaints in five categories. Deal only with reputable companies.
- Beware of companies that use high-pressure sales tactics, offer a deal that sounds too good to be true, or have sales people that lack positive identification for themselves and their company. These are "red flags" that something is not right.

Do the following before signing a contract:

- Read it carefully. Make sure you understand the protection provided by the system, equipment to be installed, initial and monthly payments, length of the contract, and the warranty period. Make sure it specifies all promises made by the sales agent. Don't be rushed.
- Have the agent explain your right to cancel the contract within three business days and how to do it. Also ask how you can cancel at the end of the contract's monitoring period to prevent an automatic renewal for another period, and what your rights are if the monitoring company is purchased or acquired by another alarm company.
- Have the agent fully explain how to operate the system, what happens if the alarm goes off, and what to do it the alarm is set off accidentally.

And do the following after signing a contract:

- Call SDPD Permits and Licensing at **(619) 531-2250** about obtaining an alarm permit. See Secs. 33.3701-33.3723 of the San Diego Municipal Code (SDMC) for burglary alarm business and agent requirements and responsibilities, alarm-user permit requirements, etc.
- Inform your insurance company. You may qualify for a discount.
- Post an alarm company sign on your property and put stickers on ground-level doors and windows.
- Check the batteries periodically and replace them if necessary.
- Call the California BSIS at **(800) 952-5210** if you have a problem with the alarm company. Or you can file a complaint online at **www.bsis.ca.gov/consumers/complaints.shtml**.

Home Cameras

Cameras are usually used just to record persons and activities in their fields of view. They can be wired or wireless. They can record continually, when motion is detected, at specified times, or on when an alarm is triggered. The imagery can be viewed on a home or remote monitor, laptop, or on a mobile device. After a crime occurs the imagery can be reviewed for usable evidence. Any camera system that is installed should be designed to provide high-quality, color imagery of persons and activities on the premises in any lighting condition for use by the SDPD in investigating crimes. And it should have backup power for at least 12 hours in the event of a power failure. Camera imagery should enable clear and certain identification of any individual on the premises. Its recordings should be kept in a secure place for at least 30 days.

Cameras can be analog or digital, i.e. Closed-Circuit TeleVision (CCTV) or Internet Protocol (IP). Imagery from both can be stored and monitored on site and viewed remotely over a secure, password-protected Internet link. Camera imagery can be used in several ways. In one, recorded imagery is stored for use in future crime investigations. In another, imagery is used as it is being recorded to report and deal with crimes in progress. However, because it is unrealistic to expect someone to monitor cameras all the time, the monitoring might be done at random times or when an alarm or alert condition occurs. Monitoring at random times is usually adequate for dealing with crimes that exist for several hours, e.g., illegal lodging on a sidewalk. Monitoring when an alarm or alert condition occurs is necessary for dealing with crimes that could occur at any time and last a few minutes, e.g., a burglary or a robbery.

Alarms can be triggered by a break-in, motion in an area covered by cameras, an open door or gate, a robbery, etc. Either CCTV or IP cameras can be used to record on alarms. Alert conditions include motion in and out of an area, an unattended object, irregular motion, objects that have moved or are missing, overcrowding, behavior, e.g., casing or tailgating, etc. Programmable IP cameras with video-analytics software, so-called "smart" cameras, are needed to record when specific conditions occur. They have other advantages over CCTV cameras. These include higher resolution, better video quality, and video encryption.

Burglars may be deterred from breaking into your home if they know that their actions will be recorded on a camera system. And if they do break in and the camera imagery can be accessed by the alarm company, personnel there can look at the imagery and see what's happening. Or it can be accessed by a web-enabled mobile device. This should be done over a secure, password-protected Internet link. If a crime in progress is seen, **911** would be

called and the dispatcher would be given the details. This will lead to a higher call priority and a faster response than would occur for an unverified alarm call. And by relaying real-time information to officers en route to the home, the officers can make better, more-informed tactical decisions in dealing with the suspects. Officers might even arrive in time to arrest them. If something suspicious is seen it would be reported to the SDPD on its non-emergency number, **(619) 531-2000** or **(858) 484-3154**. Or a security company car could be dispatched to investigate.

Systems that used to cost thousands of dollars now cost hundreds of dollars and are relatively easy to install. For example, a homeowner can now buy eight CCTV cameras and an eight-channel Digital Video Recorder (DVR) for as low as $400. A basic eight-camera system could cover the approaches to your home from the street and the doors and windows that a burglar might break in through.

Signs regarding cameras should be posted to help deter crimes. If the cameras are not monitored all the time, the signs should use phrases RECORDED VIDEO SURVEILLANCE IN USE or ALL ACTIVITIES ARE RECORDED TO AID IN THE PROSECUTION OF CRIMES COMMITTED ON THE PREMISES. Don't use words like SECURITY, PROTECTION, or MONITORING because they can give people a false expectation of an immediate security response when an incident occurs or that they and their property are somehow being protected by the cameras.

Cameras in Multi-Family Buildings

In multi-family residential buildings that don't have burglar or robbery alarms, "smart" IP cameras can be used to record unusual or suspicious activities in and around the building. Those activities can be defined by various alert conditions that can be set by day of the week and time of the day. When an alert condition occurs, the imagery can be accessed to see what's happening so appropriate actions can be taken. This could be done on the premises, at a security company office, or on a web-enable mobile device. For remote viewing, a secure, password-protected Internet link is needed for access to the imagery. If a crime in progress is seen, **911** would be called and the dispatcher would be given the details. And by relaying real-time information to officers en route to the building, the officers can make better, more-informed tactical decisions in dealing with the suspects. Officers might even arrive in time to arrest them. If something suspicious is seen it would be reported to the SDPD on its non-emergency number, **(619) 531-2000** or **(858) 484-3154**. Or a security company car could be dispatched to investigate. For example, to deal with vehicle thefts and break-ins in the building's parking facility, the software could be programmed to alert the monitoring stations when any of the following occurs: someone walks between several vehicles apparently looking for a vehicle to break into, someone loiters between vehicles, a vehicle drives up and down aisles without parking in empty spaces perhaps looking for a particular vehicle to steal, and a vehicle stops in an aisle and someone gets out and goes to a parked vehicle.

Burglars may be deterred from breaking into units if they know the units have an alarm system and their actions will be recorded on a camera system. Then if they do break in and imagery is accessed by the alarm company, personnel there can look at the imagery and see what's happening. Or it can be accessed by a web-enabled mobile device. If a crime in progress is seen, **911** would be called and the dispatcher would be given the details. This will lead to a higher call priority and a faster response than would occur for an unverified alarm call. And by relaying real-time information to officers en route to the building, the police response would be faster and the burglars might be caught before they can escape. Camera systems that used to cost thousands of dollars now cost hundreds of dollars and are relatively easy to install. For example, one can now buy eight CCTV cameras and an eight-channel Digital Video Recorder (DVR) for as low as $400. A basic eight-camera system could cover the doors and every room in a unit.

Procedures

- Lock all doors and windows when you go out, even if it's just "for a minute." Unless windows have security grilles, bars, or screens, they can be left partially open for ventilation only if secondary locking devices are used. These vary with window type, e.g., thumbscrew-type locks can be used in the tracks of sliding-glass windows.
- Lock gates, garages, and sheds after each use.
- Store bicycles, mowers, etc. in a locked garage or shed, or secure them to some stationary point.

- Don't leave a ladder in your yard. It's an invitation to a burglar to try a second-floor window.
- Don't leave notes on your door when you are away from home.
- Don't leave keys in mailboxes or planters, under doormats, or in other obvious hiding spots. Leave an extra key with a neighbor.
- Know who's at your door before opening it. Check photo registration card before dealing with any solicitors, peddlers, interviewers, etc. These persons are required to obtain a card from the SDPD and display it on the front of their clothing. They are allowed to solicit only between 9:00 a.m. and 8:00 p.m. except by appointment.
- If you don't want to open 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." Burglars often knock at the door to see if a house is empty. If you don't respond, they may think the house is empty and attempt to break in. If you do respond, they will usually go away and try another house.
- Be suspicious of persons making unsolicited offers of services.
- Post a NO SOLICITING sign if you don't want any solicitor to ring your door bell, knock on your door, or make any other sound to attract your attention. Cite SDMC Sec. 33.1407 on the sign.
- Ask for photo identification before letting in anyone you don't know. Check out the identification with the company or agency if you are suspicious.
- Never let a stranger enter your home to use the telephone. Offer to make the call yourself in an emergency.
- Don't give your name, phone number, or whereabouts on your answering machine message. Never say you aren't home. Just ask the caller to leave a message.
- Don't leave your home keys on a chain with your vehicle keys when you use valet parking. 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 a criminal is not likely to find them.
- Don't give maids, babysitters, or others working in your home access to your home keys or alarm codes.
- Call **911** if you are at home and think someone might be breaking in. Don't take direct action yourself. An officer will be dispatched to your address even if you cannot speak or hang up.
- Don't go in or call out if you suspect someone has broken into your home, e.g., if a window or screen is broken, a door is ajar, a strange vehicle is parked in the driveway, or your burglar alarm has gone off. Go to a neighbor's home or use your cell phone to call **911**. Wait for the police to arrive. Enter when they say it is safe to do so.
- Don't discuss your assets or finances with strangers.
- Don't keep large sums of money at home.
- Keep valuable papers, stocks, bonds, expensive jewelry, coin collections, etc. in a bank safe deposit box. Don't store them at home unless you have a security closet or a safe that is well hidden and cannot be removed. Or if you do keep some at home, don't keep them in the master bedroom. That's the first place burglars look and ransack. The laundry room would be a better place to hide valuables,
- Take the following additional measures to protect your valuables when staging an open house. Lock up all cash, expensive jewelry, personal and financial papers, prescription drugs, guns, power tools, etc. Have everybody entering your house show a photo ID and sign a registration sheet. Don't let anyone in unless he or she is accompanied by an agent and tell the agent not to let his or her clients out of sight at any time.

What Burglars Say

Here's what some convicted burglars say about breaking into homes.

- Of course I look familiar, I was here just last week cleaning your carpets, painting your shutters, or delivering your new TV.
- Thanks for letting me use the bathroom when I was working in your yard last week. While I was in there I unlatched the back window to make my return a little easier.
- Those nice yard toys your kids leave out make me wonder what type of gaming system they have.
- I might leave a pizza flyer in your front door to see how long it takes you to remove it.
- Don't forget to lock your doors and windows when you go out, even in bad weather. I usually get in through unlocked doors or windows. And I work in bad weather too.
- I do my best not to look like a burglar when I walk around. Sometimes I carry a clipboard or a briefcase.

- I always knock first. If you answer, I'll have some excuse for knocking, like "I'm looking for my dog." If you don't answer I'll try the door. Occasionally I hit the jackpot and walk right in. And if the door is locked, I'll try the doors and windows in the side and back yards.
- A window open a little to let in a little fresh air during the day is an invitation for me to come in. If you do that put something in the track that prevents someone from opening it wide enough to get through.
- I'll break a window to get in even if it makes a little noise. If your neighbor hears a loud sound he'll stop what he's doing and wait to hear it again. If he doesn't hear it again he'll just go back to what he was doing. It's human nature.
- I won't break into an occupied home.
- A loud TV or radio can be a better deterrent than the best alarm system. If you don't want to leave one on while you're out of town, use a timer that turns it on when you usually watch or listen to it.
- The thing I hate most is nosy neighbors.
- I don't mind barking dogs. I can quiet them with Beggin' Strips or peanut butter on bread.
- I love looking in your windows. I'm looking for signs that you're home and for flat screen TVs or gaming systems I'd like. I'll drive or walk through your neighborhood at night before you close the blinds just to pick my targets.
- Alarm company yard signs and window stickers don't bother me because I know that you might now have an alarm system, or if you do, it might not be set, and it it's set, I'll be gone before the cops arrive.
- I don't understand why you would you pay all that money for a fancy alarm system and leave your house without setting it.
- If glass is part of your front entrance, don't let your alarm company install the control pad where I can see if the alarm is set.
- If you don't alarm your windows, install motion detectors in the rooms I might enter. I usually go to the master bedroom first because that's where jewelry is usually kept and a home safe is located.
- I won't have enough time to break into that safe where you keep your valuables. But I'll take it with me if it's not bolted down.
- Do you really think I won't look in your sock drawer? I always check dresser drawers, the bedside table, and the medicine cabinet. But I almost never go into kids' rooms.
- I don't use social media for selecting targets but I know some young burglars who do. They look for posted photos of new computers, jewelry, TVs, and other valuables and then break in when the residents are away. And if they find where residents have posted plans to be away on vacation, they'd consider breaking in without seeing photos.
- A burglar who broke into over 70 homes in England, never forced an entry, and was only caught by DNA evidence said he avoided homes with any of the following:
  - A dog or sign warning of a dog
  - Burglar alarm
  - Cameras
  - Lights on inside
  - Lights outside on motion detectors
  - Barbed wire on fences and gates
  - Anti-climb paint on fences and walls

SMART HOME SYSTEMS

Home automation systems and smart phones are now available to let you make your home a smart home. With the Internet of Things (IoT), a term coined in 1999 for the concept of connecting devices with on and off switches to the Internet, you can control your home's lighting, air conditioning, appliances, and security and entertainment systems from almost anywhere. Here are some things you can do remotely.

- Arm and disarm your security system
- Lock and unlock your doors
- Receive security alerts when someone enters your home when the security system is armed
- View your camera imagery to see what's going on in and outside your home
- Talk to and look at people who ring your doorbell
- Turn lights on and off

- Turn your thermostat up or down
- Record radio and TV programs
- Turn cooking appliances on and off
- Monitor your babies

Because many of these connected devices have no security, hackers are releasing malware into the Internet to search for them and taking them over to commit crimes or paralyze businesses and government institutions. And once they find a way into your home, they can move laterally and compromise your network devices, including routers, laptops, phones, tablets, and hard drives. They can then steal your personal information, identify bank account logins and credit card numbers, send malicious and spam e-mails, etc. In an Oct. 14, 2016 release at **www.us-cert.gov/ncas/alerts/TA16-288A**, the United States Computer Emergency Readiness Team (US-CERT) suggests that users and administrators take the following precautions to prevent a malware infection in an IoT device:

- Ensure that all default passwords are changed to strong passwords, i.e., ones one that are at least 12 characters long, completely random, and have at least one capital letter, one lowercase letter, one number, and one symbol. Default usernames and passwords for most devices can easily be found on the Internet, making devices with default passwords extremely vulnerable.
- Update IoT devices with security patches as soon as patches become available. This will help keep them free from malware.
- Purchase IoT devices from companies with a reputation for providing secure devices. Set your devices for automatic updates when available.
- Know the capabilities of all IoT devices and appliances installed in your home. Before buying or using any in your home, have a solid understanding of how they work, the nature of their connection to the Internet, and the types of information they store and transmit. If a device comes with a default password or an open Wi-Fi connection, change the password and only allow it to operate on a home network with a secured Wi-Fi router.
- Understand the capabilities of any medical devices intended for at-home use. If the device transmits data or can be operated remotely, it has the potential to be infected.
- Monitor IP port 2323/TCP and port 23/TCP for attempts to gain unauthorized control over IoT devices using the network terminal protocol.
- Look for suspicious traffic on port 48101. Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor.

Here are some other suggested security measures.

- Disable port forwarding.
- Install a firewall to block unauthorized access.
- Encrypt communications.
- Install authentication mechanisms for communicating between your mobile device and the home system.
- Put all wireless routers, wireless access points, and cable modems on a Virtual Local Area Network (VLAN) that does not have direct access to or from the Internet.
- Set up a Virtual Private Network (VPN).
- Connect all devices in the home to a network separate from your PC.
- For your Wi-Fi networks, set up firewalls with strong passwords, and consider using media access control address filtering to limit the devices able to access your network.
- If your router gives you the option to set up more than one network, separate computing devices from IoT devices and spread them throughout several different networks. That way if cyber criminals break into one network, the damage they do will only be limited to the devices on that network.

Here are some tips for safe shopping for IoT devices.

- Go to Google for consumer reviews to see if your device is especially vulnerable to hacking. Type the name of device followed by the word “hacking” in the search box.

- When buying a device in a store, ask the salesperson to open the box so you can see whether the device comes with easy-to-read information about its security features. Also ask whether the device's password and username can be changed. You don't want to use it with the default words.
- Make sure the device can be updated with new software and ask how to switch on auto updates.
- Create a Google Alert that notifies you by e-mail when the manufacturer announces a security update. Go to **www.google.com/alerts**, type in the specific name and model of your device and your e-mail address, and then press the Create Alert button.

Because home routers are directly accessible from the Internet and are easily discoverable, usually continuously powered-on, and frequently vulnerable because of their default configuration, US-CERT Security Tip ST15-002 entitled *Security Your Home Network* last revised on Dec. 16, 2015 suggests that the following preventive steps be taken to increase the security of home routers and reduce the vulnerability of home networks against attacks from external sources. This Security Tip can be seen online at **www.us-cert.gov/ncas/tips/ST15-002**.

- Change the default username and password. Use a strong password and change it every 30 to 90 days.
- Change the default Service Set Identifier (SSID), which is a unique name that identifies a particular Wireless Local Area Network (WLAN). When choosing an SSID, make it unique and not tied to your personal or business identity.
- Don't stay logged onto the management website for your router. This is a defense against Cross-Site Request Forgery (CSRF) attacks that would transmit unauthorized commands from an attacker to the router's management website.
- Use Wi-Fi Protected Access (WPA-2) with Advanced Encryption Standard (AES) for data confidentiality. It's the most secure router configuration for home use. It uses 128-bit encryption for communication between the wireless router and the wireless computing device, and provides stronger authentication and authorization between the devices. If your router still uses Wired Equivalent Privacy (WEP), it should be upgraded. If you must use WEP, it should be configured with the 128-bit key option and the longest pre-shared key the router administrator can manage. However, you should be aware that WEP at its strongest is still easily cracked.
- Disable the Wi-Fi Protected Setup (WPS) immediately. It has a design flaw in its specification for PIN authentication that significantly reduces the time required for a brute-force attack to succeed. And it lacks a proper lockout policy after a certain number of failed attempts to guess the PIN.
- Limit WLAN signal emissions to the perimeter of your home. Extended emissions allow eavesdropping by attackers outside your home. Use a directional antenna and experiment with transmission levels and signal strength to limit coverage.
- Turn the network off when it's not in use. This will prevent outside attackers from exploiting your WLAN.
- Disable Universal Plug and Play (UPnP) unless you have a specific need for it. This feature eases initial network configuration but it is also a security hazard, e.g., malware within your network could use UPnP to open a hole in your router firewall to let intruders in.
- Upgrade router firmware with current updates and patches, many of which address network security vulnerabilities. When considering a router, check the manufacturer's website to see if it provides upgrades.
- Disable remote management to keep attackers from establishing a connection with the router and its configuration through the Wide Area Network (WAN) interface.
- Use your router's management website to determine if any unauthorized devices have joined or attempted to join your network. If an unknown device is identified, a firewall or Media Access Control (MAC) filtering rule can be applied on the router.

Finally, if you plan to install your own smart home security system and monitor it yourself, here are some things to consider.

- Backup monitoring by a home security company in case you are unable to answer an alert message on your smart phone
- Monitoring by a home security company when you are away from home
- Procedures and hardware to eliminate false alarms
- Acceptance by your insurance company for discounts
- Use by everybody in the home
- Easy-to-understand and actionable reporting recommendations

- Easy-to-update devices with security patches
- Voice recognition or other security measure for your voice assistant to prevent unauthorized persons from activating it

On Oct. 21, 2016 many of America's most popular websites were disrupted by a major cyberattack in which hackers used Mirai malware to hijack hundreds of thousands of unsecured Internet of Things (IoT) devices in people's homes and instruct them to flood target websites with more data than they can handle, thus shutting these websites down. (At the end September 2016, the hacker responsible for creating the Mirai malware released its source code, effectively letting anyone build their own attack army using Mirai.) Those that were shut down in these Distributed Denial-of-Service (DDoS) attacks included Twitter, PayPal, Netflix, Airbnb, Reddit, and Spotify. The attacks are call "distributed" because the attacker uses multiple computers to launch them. If your devices were not protected as suggested above, they may have been involved in these attacks. To remove the Mirai malware from an infected IoT device, US-CERT suggests that you take the following actions.

- Disconnect device from the network.
- While disconnected from the network and Internet, perform a reboot. Because Mirai malware exists in dynamic memory, rebooting the device clears the malware.
- Ensure that the password for accessing the device has been changed from the default password to a strong password. Reconnect to the network only after rebooting and changing the password. If you reconnect before changing the password, the device could be quickly reinfected with the Mirai malware.

PROVIDING VISIBILITY

- Leave outside lights on after dark or have outside lights controlled by a motion detector. Make sure there are no dark areas around the house, garage, or yard in which a person could hide. Street lights are generally inadequate for illuminating your property.
- Check lights regularly and replace burnt out bulbs.
- Trim bushes to less than 3 feet to eliminate possible hiding places, especially near windows and sidewalks.
- Trim tree canopies to at least 8 feet to allow visibility into your property. Homes that are hidden from the street and the neighbors are more likely to be burglarized.
- Replace solid walls in front yards with open fencing to eliminate hiding places and make climbing more difficult.
- Install a wide-angle peephole in your front door so you can look out without being seen yourself.

MAINTAINING YOUR PROPERTY

- Keep property in good condition and free of trash, litter, weeds, leaves, graffiti, dismantled or inoperative vehicles, and other things that indicate neglect in caring for your property.
- Replace broken windows or screens.
- Repair broken fences and gate locks.
- Use screens, wired glass, or other protection for light fixtures and bulbs.
- Remove loose rocks and other objects that could be used to vandalize your property.

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 call **911** to report it.
- 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 Station to request vacation home checks when you'll be out of town.
- 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 their 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 property.

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**.

In addition to filing a Letter of Agency as described above, a property owner facing continuing crime problems on his or her property can submit a Citizen Request Form by going to the Forms page on the SDPD website at **www.sandiego.gov/police/forms/forms**, clicking on Citizen Request Form, filling out the Form online with as much information as possible about the problem, and then clicking on the Submit Request button at the bottom of the Form. You can use this Form to request additional patrol and/or to report criminal activity at a specific address. It will be sent to the responsible Division for review and response as appropriate.

HELPING TO PREVENT RESIDENTIAL BURGLARIES IN YOUR NEIGHBORHOOD

The tips in this section apply to apartment and condo communities as well as neighborhoods. First, join or consider forming a Neighborhood Watch in your area. This program has become one of the most effective means of fighting crime in our communities because you and your neighbors are the ones who really know what is going on in your area, most likely to be the first to see a crime and call for help, and are in the best position to do the following.

- Report code violations, unsafe street conditions, etc. that degrade the quality of life in your area
- Take property owners to small claims court to abate nuisances
- Keep your block clean and free of graffiti
- Provide a safe environment for your children.

A paper that defines Neighborhood Watch and explains how to start and maintain a program in your area is available on the SDPD website at **www.sandiego.gov/police/services/prevention/programs**.

Without Neighborhood Watch, you should learn the following:

- Who belongs in your neighborhood, i.e., residents, children, friends, workers, guests, etc.
- What vehicles your neighbors drive
- When your neighbors are usually away from home
- When your neighbors are away on vacation
- When dogs usually bark
- When meter readers usually come

You can help stop a burglary in progress by promptly calling **911** if you see a person doing the following:

- Ringing the front door bell, trying to open the door, and then going into the side or back yard
- Entering a neighbor's home when the neighbor is away
- Forcing an entry of a home
- Removing property from a home, especially if the residents are away
- A neighbor screaming or calling for help

You can help prevent a possible burglary by promptly calling **(619) 531-2000** or **(858) 484-3154**, the SDPD non-emergency numbers, to report anything suspicious in your neighborhood. Examples of suspicious activities can be found in the paper entitled *Reporting and Providing Information about Crimes and Suspicious Activities* that can be opened on the Community Resources and Responsibilities page of the SDPD website at **www.sandiego.gov/police/services/prevention/community**. They include the following:

- The sound of breaking glass, an alarm, or a barking dog in a neighbor's home when the neighbor is away
- A person soliciting without a license, not displaying a valid registration card, or operating between the hours of 9:00 p.m. and 8:00 a.m.
- A person going door-to-door on your street
- A person loitering in the near a home, especially if the residents are away
- A person sitting in a parked vehicle
- A vehicle driving slowly on your street or circling your block

If you have any information that might help solve a burglary and lead to the arrest of the burglar, call your local SDPD Division Station and ask to speak to the detective handling the case. Or you can call Crime Stoppers at its 24-hour hotline at **(888) 580-8477** and provide information anonymously. Crime Stoppers is a citizen-operated, non-profit organization that works in partnership with local, state, and federal law enforcement agencies to help solve serious crimes. It gives community members an opportunity to fight crime without "getting involved." The operator there will take your information and give you a code number. If your information leads to an arrest you could earn a reward of up to $1,000. The operator will explain how you can use your code number to give additional information and how to collect your reward. Or you can provide tips by text messaging from a cell phone to **274637** with **SDTips** at the beginning of the message.

You can also provide tips from TipSoft by Public Engines on its website at **www.tipsubmit.com**. Web, mobile, or text tips submitted from it are encrypted, entirely confidential, and completely anonymous. They are immediately and securely transferred directly to Crime Stoppers that use the TipSoft Tip-Management application.

MAKING SURE THE POLICE CAN FIND YOUR HOME

- Make sure your street address number is clearly visible from the street and is well lighted at night so the police and other emergency personnel can locate your home easily. Numbers must be at least 6 inches high on individual dwellings and duplexes, and 12 inches high on multiple-unit residential buildings.
- Make sure your unit number (in a multifamily housing development) is clearly visible from paths in the development. A directory or map that shows paths and unit locations should be placed at the main entrance of the development.
- Provide the police with an entry code if you live in a gated community.

IDENTIFYING YOUR PROPERTY

- Etch your driver's license number on any valuables that might be stolen.
- Photograph valuables that cannot be etched.
- Keep a detailed, up-to-date record of your valuables. Include type, model, serial number, proof of purchase, and fair market value.

PREVENTING EMPLOYEE AND CONTRACTOR THEFT

Despite your best efforts, dishonest employees can usually find ways to steal. If you suspect theft, call the SDPD at **(619) 531-2000** or **(858) 484-3154**. Don't play detective and try to solve the crime. And don't jump to unwarranted conclusions. A false accusation could result in serious civil liability.

Conduct a thorough background check before hiring a housekeeper, nanny, or other person who works regularly in your home. Consider using an outside company to collect information. Checks should be made for criminal arrests and convictions, outstanding warrants, bankruptcies, credit problems, civil judgments, citizenship, etc. And past employment should be verified. Some checks should be made annually.

In selecting a contractor to work in or outside your home you should check its references and make sure it is insured and bonded. Insurance will protect you from damage caused by the contractor's employees. A surety bond will guarantee that the work will be performed as stated in the contract. For some contractors you can require a bond that will cover theft or other losses resulting from dishonest acts committed by an employee acting alone or in collusion with other persons. Some bonds require that the employee be prosecuted and convicted of the crime. Others require evidence of employee dishonesty. The conditions for coverage would be negotiated in drafting the bond.

You should also check that the contractor is licensed to work in the City of San Diego, i.e., that it has a Business Tax Certificate. This can be done on the Master Business Listing page of the City's website at **www.sandiego.gov/treasurer/taxesfees/btax/nblactive.shtml**. Construction contractors should be licensed by the State of California. You can check the status of a contractor's license on the Contractors State License Board's website at **www2.cslb.ca.gov/OnlineServices/CheckLicenseII/CheckLicense.aspx**.

You can also require that the contractor conduct a background investigation on each employee that will work at your home. For this you will need to specify the following: (1) information an employee will have to provide, e.g., personal history, references, fingerprints, etc., (2) kinds of checks to be made, e.g., employee's name and SSN, criminal history, DMV record, credit record, civil action history, etc., and (3) criteria for passing each check, e.g., no criminal convictions or outstanding warrants, no bankruptcies, no civil judgments, etc. The contractor should also be prohibited from substituting a cleared employee with one that is not cleared, or subcontracting any of the services.

Take additional measures to protect your valuables when workers are in your home. Lock up all cash, expensive jewelry, personal and financial papers, prescription drugs, guns, easily movable tools, etc. Also, ask each contractor and sub-contractor to provide a list of everyone who will work in your home. And for each worker, keep a record of the days and hours they are in your home along with their names, addresses, phone numbers, and driver and vehicle license numbers.

The opportunities for employee theft can be reduced by having the contract work done when you are home. This is the best option. Otherwise you'll have to give the contractor's employees means to enter your home when you are away, i.e., keys, door codes, or individual access cards, as well as the codes to any alarm systems that are installed. And the employee will have to lock all doors and turn on the alarm(s) when he or she leaves.

SDPD DIVISION STATIONS

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