

# **COMMERCIAL SECURITY HANDBOOK**

**APPLYING**

***CRIME PREVENTION THROUGH***

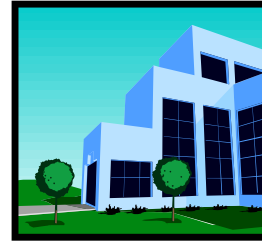
***ENVIRONMENTAL DESIGN* Concepts**



**San Diego County  
Sheriff's Department  
Crime Prevention Unit**

# Introduction

---



The purpose of the *Commercial Security Guide* is to help:

- **identify** common commercial crime problems.
- **define and identify** recognized commercial crime prevention concepts.
- **suggest** methods for implementing commercial crime prevention solutions.

## Commercial Crime

Common problems challenging commercial crime prevention include:

- burglary and theft of property
- robbery and its potential for more violent crimes
- identity theft and compromising personal information of customers and employees
- theft of property, goods, services or information from internal and external sources.

Each industry faces specific variants of these crimes. Security measures can decrease insurance costs, reduce potential liability, and reduce losses.

## Crime Prevention Through Environmental Design

Most law enforcement agencies promote the principles of Crime Prevention Through Environmental Design (CPTED) as the most effective way to confront crime. This holistic approach incorporates **access control**, **territorial reinforcement**, **natural surveillance**, and **maintenance**.

**Access Control**- By designing elements of the exterior to guide access by people (customers), one can deter access to potential targets of crime. Anything out of the ordinary would be easily noticed and reported to law enforcement. Eliminating secluded areas and providing adequate lighting at night can discourage criminal activity.

**Territorial Reinforcement**- This concept uses the exterior design to show that the property is owned and enlists territorial reinforcement strategies. Specific landscaping, adequate lighting, strategic walkways, decorative fencing, and clear signage indicate that trespassers are not welcome.

**Natural Surveillance**- This common-sense method offers little opportunity for a would-be criminal to succeed because of the high visibility of all sides of the property. Open staircases, well-lit parking lots and the interiors of buildings, and trimmed landscaping discourage crime. Also, businesses that are located in a mixed-use area of residential and commercial building have a decided advantage.

**Maintenance**- It is an important message that a well-maintained property sends to a potential criminal: the owner takes pride in the neighborhood and takes responsibility for his/her property. Positive attitudes manifest themselves in immediate graffiti removal, landscape maintenance, and on-going repair of buildings.



# Implementing Crime Prevention

The contents of this *Commercial Security Guide* suggest effective and efficient solutions to commercial crime prevention problems. Among the topics included are:

- **Physical Security** issues, such as lighting, alarms and landscaping.
- **Robbery Prevention** techniques, including an employee training guide.
- **Shoplifting Prevention** strategies (for both amateurs and professionals).
- **Frauds and Cons** warnings about cash transactions and check and credit card abuses.
- **Internal Theft Prevention** tips.
- **High-tech Crimes**, including theft of property, services, and personal information by surreptitious intrusion into sensitive files by computer or other electronic means is described.
- **Terrorism, Arson, and Vandalism** issues.
- **Personal Safety for Employees.**
- **Business Watch**, an effective collaboration of law enforcement and the business community.

# Burglary

---



## Lighting

Most commercial burglaries occur at night. Because darkness can conceal a burglar, it is necessary to provide high visibility by flooding all sides of your buildings, parking lots, storage areas, and trash depositories with adequate lighting. Protective lighting priorities begin with perimeters and vulnerable areas or structures.



Exterior lighting usually needs lower intensity than interior spaces. San Diego Gas and Electric ( [www.sdge.com/index](http://www.sdge.com/index) ) has a dusk-to-dawn program designed to help businesses use lighting in an efficient manner. Contact them for more details.

Security lighting should:

- discourage unauthorized entry.
- enhance detection of intruders.
- detect and prevent internal pilferage.

Additional considerations include stand-by lighting, maintenance, and periodic testing of systems. Replace or repair inoperative lamps immediately.

Several types of **light sources** are available:

*Incandescent or halogen lamps* live short lives and are fairly expensive to operate. The advantages are that they produce a bright light, are easy to control, and are compact.

*Florescent lamps* are less expensive to operate than incandescent or halogen and last longer. Though they put out a good light, they are more difficult to direct.

*Mercury vapor lamps* require fewer fixtures to illuminate an area, but have a shorter life. They provide excellent light, are easy to direct, control, and they are compact.

*High-pressure sodium vapor lamps* require fewer fixtures and have a low operating cost; however the fixtures themselves are expensive. They are an excellent light source, are easy to direct and control and are compact.

*Low-pressure sodium lamps* are the least expensive to operate. The fixtures themselves are expensive, but few are required. They are easy to direct and control but produce a yellow light-reducing clarity. They are longer in size. These yellow lights are often used to prevent loitering.

**Caution: Check local “light pollution” regulations before attempting any installation.**

## Addresses

Illuminate your building to facilitate emergency response. Address numbers should be easily read from the street at night (lit or back-lit numbers are the best). The rear of your business should also be identified. Numbers should be clearly mounted against a contrasting color and should measure at least 5 inches. The rear of your business should also be identified.

Placing addresses numbers on the rooftop can aid helicopter patrol.

## Landscaping



Keep plant growth from obscuring doors and windows to allow maximum visibility and better security. Consider using security plants (those with prickly leaves or thorns) as a natural barrier to intruders. They are most beneficial when planted below windows and along fence lines.

## Protective Barriers

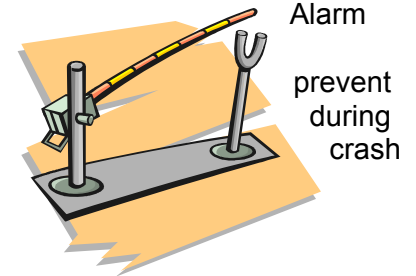
Creating protective barriers incorporates three concepts of prevention. The first is to *prevent entry*, except at controlled areas. The second is to *prevent exiting*, except through controlled points. The third goal is to *prevent access* to certain buildings or areas within the property. These three concepts can be implemented with a system of barriers in layers. Protective barriers do not always require fences, since natural barriers are often available.

### **Gates and Fences**

Sturdily built gates and fences are the first line of defense against illegal or unwanted entry. Fences should be the *maximum allowable height* with the base set in concrete around the entire perimeter. Normally, chain-link and wrought iron fences and gates provide the most cost-effective long-term systems. "Open" types of fencing also permit observation of activity within the fenced area and deter graffiti vandals. Increased security can be obtained with "top-guard" fencing. If you are considering installing an overhang of barbed wire fencing, check your local ordinances.

Control access at entrances and exits. Secure all gates with high-security locks and **use them**. When not in use, keep all padlocks in the closed position to prevent their removal. Alarm systems are available for fences.

Mount all gate latches with carriage bolts. Weld nuts or strip threads to nut removal. Access-control gates are available to restrict entry and exit business hours. Some techniques for controlling vehicle access include beams, sliding gates, and tire shredders.



### **Restrict Building Access**



Keep stackable items stored in a locked area and away from the building to avoid theft of tools, pallets, and ladders that could be used to aid a burglar. Secure ladders attached to the building with locked ladder covers.

If your building has large windows or weak walls, install bollards to prevent "smash-and-grab" drive-through burglaries. Bollards allow unrestricted pedestrian, bicycle, and wheelchair traffic, while impeding cars and trucks.

Do not overlook utility openings such as sewers air and water intakes, roof hatches and skylights, storm drains, exhausts, and others that breach the perimeter or building structures. A good guideline is to protect any opening more than ten inches. You may need heavy screening (16-gauge sheet metal or stronger), chain-link fencing welded or bolted in place, or welded-in hardened bars or pipes.

Reminder: Trash bin areas should be well lit, away from buildings and **locked**.



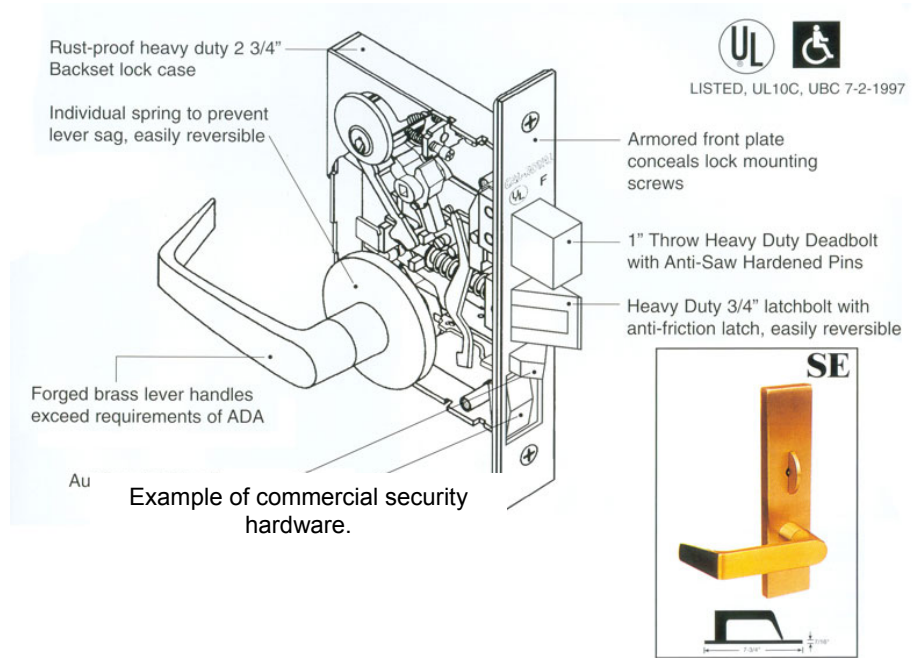
If your building is located within a complex, chances are that you share a common attic or hollow walls that make it easier for a thief to move between offices. This means **your security is only as good as your neighbor's**. Seal off or alarm these areas with motion sensors to detect intruders and encourage your business neighbors to also use the security practices recommended in this *Guide*.

## Doors

All exterior doors should be solid core. Mail slots in doors compromise security and should be sealed.

### Dead-bolt lock specifications for commercial doors:

- Throw should be at least one inch.
- Cylinder guard should be tapered
- Case trim should be steel, bronze or solid brass
- Locking mechanism should have a five-pin tumbler.



Panic deadbolt hardware is available to secure secondary exits. A panic deadbolt push-bar is advisable. These devices are a combination of a door knob or push-bar and a dead-bolt, where the dead-bolt is released when the knob is turned or the bar is pushed. These are available with alarms and without exterior keyways.



For single glass doors, swing locks should be of case-hardened steel with steel or ceramic inserts and a throw at least 1 3/4 inches.

Double doors should have three-point panic flush bolts installed on both doors. It is important that the bolts have at least a one-inch throw and are made of steel rather than nylon.

Astragals or latch-guards attach to exterior doors to protect the locking bolt against prying.

A 180-degree viewer should be installed  on all delivery, alley, and back doors.

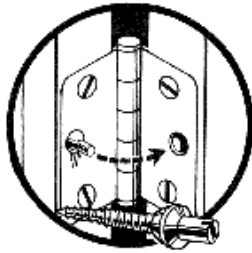
4-inch strike plate with 3-inch



With all locks, use high security strike plates with three-inch screws anchoring securely into the wall stud. Metal door reinforcements provide even greater protection against kick-in attacks. Ensure full throw of the bolt is in its receptacle.

*Exposed hinge pins* can be easily removed by a burglar and the door opened from the hinge side. Here are ways to secure ways to secure the hinge pins:

- Install commercially-made secured hinges.
- Spot-weld the hinge-pin to the hinge.
- Pin the hinges.



**Pinning Hinges**  
Insert long screws or duplex nails into the door jamb just above each hinge. Allow each to protrude about 1/2". Close the door until the screw or nail comes in contact with the door. Drill a larger hole into the door at the points of contact.

*Security screen doors* offer good protection and allow for ventilation. Insist on the following features:

- Ring guard for the single cylinder dead-bolt lock.
- Perforated or expanded metal screen to prevent reach-through.
- Steel frame installed using non-removable screws or welded in place.



## Windows

Do not rely exclusively on the hardware or locking devices supplied with your windows. Supplemental security measures are advisable. Regularly check all window security hardware and frames for corrosion and windows that have "settled" and prevent the locking latches from functioning properly.

### **Aluminum Sliding Windows**

Inspect your aluminum sliding windows to see if they have a metal or wood anti-lift strip in the upper track to keep the panel from being lifted out when in the locked position. If not, install metal screws in the upper track to prevent the windows from being taken out. To prevent the windows from being forced to slide horizontally, install an anti-slide bolt or a fitted dowel. You can also use a simple thumb-turn screw lock (the type that has a point at the end rather than the flat ones), drilling holes in the track to accommodate the screw for better security. Windows and doors left open for ventilation or for pets to access offer an invitation to would-be burglars.

### **Double-hung Windows**

It is possible for a burglar to pry open the latches on the older double-hung windows. This type of window can be secured by drilling a downward sloping hole into the top of the bottom window through and in to the bottom of the top window and inserting a pin or thick nail. Check the latch to make sure it is functioning and locking properly.

### **Vinyl Double-Paned Windows**

Do not drill into the vinyl frame of the newer vinyl double-paned windows as they are filled with an inert gas. In the likelihood that the seal would be nicked when the frame is drilled, the gas would escape and the window would begin to fog. Any drilling or modification to a "green window" would void the warranty. These windows are usually secure when the integrated locking hardware is used properly and are often equipped with "ventilation stops." It should be stressed that, as with all openings, these windows should be closed completely and locked to ensure maximum security.

## Crank Windows

People who have older homes with crank windows should ensure that the frame has not decayed and that it is in good condition. The cranking device and latch should be inspected to make sure that it is functioning properly. The latching devices can be replaced with one that has a hole on the inside. Through this hole, a pin (not a lock) can be inserted to secure it in the closed position.

## Louvered Windows

Louvered windows are especially vulnerable because the individual panes can easily be removed. This can be discouraged by removing each pane, running a bead of glue down each side, then reinserting them into the slots. We highly recommend replacing louvered windows for optimal security.

## Interior

### Visibility

Do not crowd windows with posters or displays. In addition to adequate exterior lighting, keep lights on in the interior during hours when the business is closed.

### Annunciators/Mirrors/CCTV



Surveillance devices serve as deterrents. They also create awareness and thereby discourage criminal activity.

*Annunciators* alert store personnel to entry and exit of customers and patrons. *Convex mirrors* help to reduce

shoplifter's opportunities. *Closed circuit television (CCTV)* reduces the likelihood of robbery when placed in register area.



### Alarms

Burglar alarms are an excellent investment in protection. Consult a reputable alarm agency for your needs. Advertise your security to would-be thieves. An adequate system for detecting intruders will include these four elements:

1. **Sensors-** Sensors detect a change in conditions and include:

- Switch sensors, which may be magnetic, mechanical, mercury-filled or wafer-type switches.
- Duress alarms ("panic buttons")
- Photoelectric sensors detecting changes in available light or in projected beams or lasers.
- Metallic foil sensors on breakables
- Pressure mat sensors
- Stress detectors connected to structural elements
- Vibrations sensors
- Sound-monitoring sensors

Motion sensors may be infrared, microwave, ultrasound or Doppler-effect.

Remember: Sensors cannot distinguish between **authorized** and **unauthorized** entry.

2. **Controls-** Controls receive information from sensors, evaluate it, and transmit the result to the annunciator device (s).



3. **Annunciation-** The electronic signal passed on by the control device alerts a human monitor. The monitor may be on site, as a security guard or a resident, but it is usually off-premises in a distant monitoring station, sometimes out-of-state. The annunciator may be a bell, siren, buzzer, or complex computer output.
4. **Response-** While an alarm may scare off a potential intruder, and the mere presence of a detection system may ward off some intruders, no alarm system is complete unless someone is alerted to investigate the cause of the alarm.

Your decision about an intrusion detection system should include consideration of the following factors:

- ▶ How well the system meets your specific needs.
- ▶ The value of the property being protected.
- ▶ Environmental factors of construction, ambient noise levels, climactic conditions, radio, and electrical interference.
- ▶ Availability and response times of monitors.
- ▶ Types of threats likely to be encountered (burglary, vandalism, sabotage, espionage, etc.).
- ▶ Employees' ability to operate the system correctly to avoid false alarms.
- ▶ Be sure to research and understand local codes and penalties relative to false alarms.

### Safes

Decide whether your circumstances require a *fire safe* or a *burglar-resistant safe*. For any safe:

- ▶ Bolt or anchor to the floor.
- ▶ Keep in a low-profile area
- ▶ Restrict access to keys or combination.



### High-security operations

An important element of your overall security program is the protection of sensitive areas within your structure(s). *Computer centers, information storage areas, research and development centers, cash depositories, security offices,* and other operations may be located within high-security “structures within structures.” Consider the following factors:

- ▶ Physical location within the building.
- ▶ Access control-both interior and exterior access, including large heating and cooling ducts.
- ▶ Power source security.
- ▶ Fire prevention and procedures-especially unwanted activation
- ▶ Disposal procedures of printed data

# Robbery


Robbery is the unlawful act of taking personal property from a person or in his presence, by force or fear of injury. Robbery is a violent crime. This may include the use of a weapon. Robbers often case the area for likely victims. Take measures to make your business less tempting to robbers. Keep in mind, would-be robbers look for these elements: *surprise, lack of witnesses, and cash on hand.*

means



**To avoid becoming a robbery victim, you must stay alert to your surroundings and customers and use common sense.**

## REDUCE YOUR RISK!

- Keep windows and counters clear-not cluttered with signs and displays.
- Situate the cash register so that it is visible from the outside.
- Use a **drop safe** and keep very little cash at the register. Always keep your safe locked when access is not required.
- Display signs indicating that employees don't not have access to the safe.  

- Be unpredictable about moving money from the business to the bank. change time, routes, and methods of concealment. if you use an armored car service, always be prepared for their pick-up and delivery.
- Keep doors that lead to unauthorized areas locked!
- **Never re-open** your business for anyone after you have closed! Be wary of the caller who states that your business has just been broken into and asks you to come down. Always confirm (by calling back) that the call was from a law enforcement agency or your alarm company before entering your business.
- **Avoid working alone.** If you must, keep a television or radio playing in the backrooms to suggest that someone else is presence.
- **Use "bait money"!** List serial and series numbers and keep them separated. Do not use these bills to make change.
- Well-trained, highly visible security guards can be a deterrent for robbers.
- Train your employees about what to do during a robbery.
- **Know what is happening outside the store.** Post "No Loitering" signs. Look for anyone watching the store or acting suspicious. Make sure that exterior lighting is adequate.
- Install a hold-up alarm surveillance camera. Use highly visible signs to advertise your security system.
- **Record** descriptions of suspicious persons or vehicles.
- **Be alert** to your customers and surroundings, especially at opening and closing. Two employees should open and close, if possible.
- **Greet all customers**, making eye contact as they enter the business. Ask if they need assistance. Customers and clients like attention; robbers do not!
- Move away from the register when there are no customers at the sales counter. Lock the register when it is unattended.
- Find out whether you are obligated to allow customers to use your restrooms. Different establishments have different policies.
- Place colored height marks at all exits to estimate a suspect's height.
- Develop a mutual aid system with neighboring merchants to keep an eye on each other's businesses and watch for suspicious activity. An inexpensive buzzer system can alert adjoining businesses to an emergency situation (see "*Business Watch*").

# Robbery Training Guide



Remember that every robbery situation is different. You will need to assess yourself, the robber, and the situation to determine what you should do. With that in mind, here are some tips:

## ACT CALMLY.

By acting calmly, you may avoid a more dangerous situation.

Do exactly what the robber says. Keep your movements short and smooth to **avoid startling** the robber.

If you remain calm, you will be better able to provide an accurate description.

## DO NOT RESIST!

Cooperate for your own safety and the safety of others. Robbers usually are excited, and may be high on drugs, and are easily provoked. Tell the robber about any possible surprises, such as movements you may have to make or that someone is in the back room, etc.



Try to give him bait money if this can be done without his knowing.

Activate an alarm only if it is silent and can be done surreptitiously. Know how to activate it by touch.

## OBSERVE CAREFULLY!

You will have less than two minutes to:

- Study his face.
- Remember his clothing.
- Note the direction of travel.
- Obtain the license, color, and make of the car (if it is safe to do so).



Use the information on the "Suspicious Activity" brochure to help you with your recollection.

## AFTER THE ROBBER LEAVES, IMMEDIATELY:

- **Lock the door.** Discontinue regular business until deputies have searched the scene.



- Call **9-1-1**.

- If you **act quickly**, the robber may be apprehended. Call law enforcement before you call the owner or anyone else.

- **Preserve the scene.**

Cover any surfaces the robber may have touched and keep away from areas the robber may have been.

Ask witnesses to remain. If they are unable to stay, get names and phone numbers. Verify with their driver's license or ID.

- Complete the suspect information form. **Write down** everything you can remember about the robber and the crime itself.



- **Do not discuss** the robbery with others until all statements have been taken.

- **Testify** in court to prevent others from being victimized in the future.



# IN CASE OF ROBBERY DIAL 9-1-1



Vehicle description: \_\_\_\_\_  
(license number, color, type, make)

\_\_\_\_\_

Direction of travel: \_\_\_\_\_

What robber said: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Companions: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Sex _____	Hat _____	Marks _____
Age _____	Coat _____	Tattoos _____
Race _____	Shirt _____	Scars _____
Piercings _____	Accessories _____	

# Shoplifting

---

Shoplifting can cost your business thousands of dollars each year. Shoplifters may be any age, sex, economic or ethnic background. There is no “typical” shoplifter. Often they work in pairs or groups to divert clerks’ attention while they steal. Certain times of the day, when employees are apt to be less alert, are critical: store opening or closing, as well as during lunch, dinner and shift changes. Shoplifters learn to take advantage of crowded stores during peak hours. Effective prevention begins with an aware and alert staff.

## PROTECTIVE MEASURES

You can begin to combat the shoplifting problem by establishing effective deterrents within the store. Preventive measures must accomplish two goals: to heighten a shoplifter’s feeling of being watched; and to minimize potential shoplifters’ access to merchandise without inconveniencing customers.

Post placards warning against shoplifting and the consequences: that you will and do prosecute.



The best way to discourage shoplifters is by taking a “get tough” attitude and prosecuting even on the first offense. *Keep your business from being tagged an “easy mark.”*

Watch for customers with loose or baggy clothing inappropriate for the weather, large bags of other props such as newspapers, strollers, briefcases, or umbrellas. These items can easily conceal merchandise. Consider checking patrons’ parcels upon entering the store.

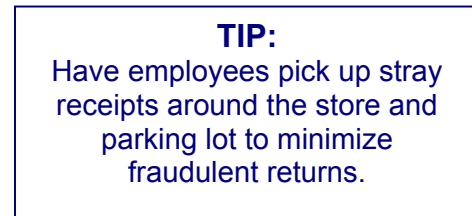
Both amateurs and professionals employ similar strategies to confuse and distract clerks. When working in teams, one of the suspects creates a disturbance, such as loudly complaining, staging a medical problem, or knocking over a display, while the accomplice works without being noticed.

Attentive sales associates who are trained to be helpful and enlist customer service techniques, especially toward a suspicious

patron, can reduce shoplifting incidents. Acknowledging each person with a “May I help you?” or “I’ll be with you in a minute,” warns a potential thief that he/she is being watched.

Cashiers familiar with store prices help curb the “price switch” method.

Merchandise return policies should require a receipt for cash returns. Require an ID and signature for returns without a receipt. Offer store-credit-only vouchers.



Returned merchandise should be inventoried against receipts on a regular basis to catch false returns (return transactions without returned merchandise).

## DISPLAY STRATEGIES

Keep display and clothing racks away from doorways and exits to discourage “hit and run” thieves. Alternate hangers front-to-back to deter thieves from grabbing bundles of display merchandise.

*Keep small and expensive items out of reach or in locked display cases.* The stores most vulnerable to shoplifters are those that sell small, concealed items such as jewelry, hardware, clothing, drug stores, department and variety stores. Show only one item at a time and wait on only one customer at a time.

Showcase items may justify the need for *special glazing material*. Display cases are particularly vulnerable to smash-and-grab attacks. The use of laminated glass can provide additional protection. Also, secure the display case doors with appropriate locks.

*Elevate* the register operator's platform and arrange displays to create maximum visibility.

Display merchandise should be neatly arranged to *detect any missing items*. Daily or weekly inventory is useful to detect loss or pilferage.

Garments can be protected with padlocked chains or electronic sensor tags which emit noise when taken out of the store illegally. Some deterrent kits will "ink" clothing and the shoplifter when pried or damaged.

### FITTING ROOM SECURITY

Keep fitting room doors locked when not in use. Café doors allow monitoring by the staff.

Limit the number of items that a customer can take into the dressing room. Be wary of customers who bring in other large bags.



Use a return rack for unwanted items.

Post signs clearly stating your policy on shoplifting.

### PRICE TAG-SWITCHING

Deter ticket-switching by...

- ...using tamper-proof gummed labels.



- ...attaching tags with plastic string that is difficult to break
- ...using only pre-printed (never hand-written) price tags.
- ...using concealed multiple price tickets.

### SURVEILLANCE

Surveillance devices are only good if they are used correctly and consistently. Most shoplifters will "case" your store for its layout as well as for security devices, which may ultimately deter him/her from actually committing the crime.



One-way mirrors from the office out to the sales floor can alert employees to shoplifters.

Convex or corner-mounted mirrors can eliminate blind spots. It is essential to keep them clean for better visibility. Employees should make it a habit to glance at them often.

Closed Circuit television (CCTV) works best when customers know that you have it. Mounted in the ceiling in strategic areas, it can deter thieves and dishonest employees.

Consider mounting a monitor in plain sight near the register to deter a possible crime.

Video-taped surveillance can help identify and prosecute suspects.

Uniformed guards are also powerful visual deterrents.

### EDUCATING EMPLOYEES

Train your sales staff to be alert to the shoplifter's early warning signals. They should look out for customers carrying concealment devices.

They should watch for shoppers walking with short or unnatural steps, tip-offs that the customer might be hiding items.



Cashiers should be trained to check the lower racks of shopping carts, to watch for switched price labels, to inspect retail items which could double as containers for shoplifters (tool boxes, jacket sleeves, covered boxes), and to check for factory seals on boxed items (checking inside if not factory sealed).

They should pay special attention to a customer who handles a lot of merchandise and takes an inordinate time to make a decision. Watch also for customers lingering in one area, loitering near stock rooms or other restricted areas, or wandering aimlessly through the store. Try to be alert to customers who consistently shop during hours when staff numbers are low.

There are several ways to identify merchandise as having been purchased. One is to instruct sales associates to staple receipts to the outside of packages. Another is to use electronic tags which are removed or desensitized at the register.

Periodic or quarterly review sessions on store policies will help keep employees alert.

You can help your employees help you. Schedule their working hours to allow an adequate number of clerks to be on hand at all times. Discourage socializing on the sales floor. A group of employees in one spot means inadequate coverage somewhere else.

**FOR A CRIME IN PROGRESS or if the suspect is still present, CALL 9-1-1**

## **TO PREVENT SHOPLIFTING**

- Provide good customer service.
- Cover the sales floor at all times, including the front door and blind spots of the store.

- Be aware of what's going on in your store. Alert store personnel and/or security immediately when any suspicious behavior is observed. Shoplifters take advantage of a crowded store during peak hours and inexperienced personnel during hectic holiday periods.

## **THINGS TO LOOK FOR**

- Watch customer's eyes. Shoppers look at merchandise. If they are looking at you or scanning the store, they might be thinking about shoplifting.
- There is no such thing as a "typical shoplifter." Watch for customers with loose or baggy clothing, large bags or purses, or other "props" that can easily conceal merchandise.
- Be aware of customers who seem nervous or refuse assistance.
- Make note of customers who visit the store frequently, but only make token purchases.
- Be alert for disturbances which may be staged to distract store staff while an accomplice steals merchandise.
- Be aware of people shopping in groups.

## **STOPPING A SHOPLIFTER**

- If you suspect that someone may be considering shoplifting, approach the customer if possible and ask, "Would you like to pay for this now?"
- If you suspect a shoplifter, keep him or her in sight and notify your manager or security personnel immediately. If you are working alone, request assistance of a next-door worker. Have a contact-plan in place before the need arises. Do not try to physically apprehend a suspect, especially if he makes a threat to physically harm you.
- Check state laws concerning apprehension of shoplifters. Your attorney can help you. Information is also available through the California Attorney Generals Office and the U.S. Small Business Association.

# INTERNAL THEFT

---

Employee theft is far more common than thought. A retail industry study showed more than one-third of thefts was by employees.

One way of controlling theft is to develop a greater commitment among your employees to your firm, have them feel respected and rewarded for doing the job well.

Providing career opportunities is also important. Companies with the lowest turnover were found to have the lowest theft rate.

## EMPLOYEE PILFERAGE

Adopt strict policies. Distribute to all employees in writing.

Take every precaution to ensure that the people you hire are honest to begin with. Run a thorough reference check to screen all applicants prior to hiring.

Applicant screening services are available. Paper-and-pencil tests can help predict honesty. Studies show that simply lengthening the hiring process (such as more interviews) helps increase new-hire loyalty.

Inform employees that they can be caught. If you have good surveillance and security measures, let them know. Many employees steal because the temptation is too great.

Personal property and purchases should be stored and locked while working.

## RETAIL SALES

Make routine “spot” checks on inventory and merchandise.

New employee should never be allowed to wear or use merchandise without

purchasing it. Purchases and receipts should be inspected at the beginning or end of shift.

Employees not scheduled to work should not be allowed to be in the business before or after business hours.



Do not permit employees to ring their own purchases.

Keep a record of all employee purchases, exchanges, or refunds.

Do not allow visitors in restricted areas.

When it is necessary for non-employees to enter restricted areas, they should be accompanied by an authorized employee.

If practical, keep trash bins secured. Inspect trash bins regularly for merchandise that could be picked up later by dishonest employees. Use clear plastic bags for trash disposal.

Insist that trash is not always removed by the same employee. If possible, employees should work in pairs or have management inspect the contents.



## PURCHASING PROCEDURES

Centralize the purchasing function, but separate from receiving and accounting.

Control purchase orders by pre-numbering in sequence.

## RECEIVING PROCEDURES

Secure the area where merchandise is received.

Count or weigh all incoming material.

Alternate the two people assigned to verify shipments.

## INVENTORY CONTROL

1. **Conduct inventories often** and at irregular intervals. Inventories can be self-conducted, completed by inventory services or by purchase orders (Point of Sale)
2. **Set a policy** that establishes a climate of accountability.
3. **Inform** all employees during orientation that inventories and spot-checks are conducted.

**TIP: IF EMPLOYEES WEAR UNIFORMS, DO NOT PROVIDE POCKETS.**

## CASH HANDLING

Every transaction must have a receipt! Encourage customers to expect a receipt by adopting a policy and posting signs at each register.



One employee should be in charge of setting up cash drawers; another should double-check the cash counts.



Ideally, each employee should be responsible for his or her own cash drawer; i.e. one drawer per on-duty employee. No other employee should at any time be allowed to open or use another's drawer. At the end of a shift, each cash drawer should be balanced by the employee and double-checked by another.

Require closing the cash drawer after each transaction.

Never leave a register unlocked when not attended. Take register keys with you. Keep the register drawer closed when not conducting a transaction.

Verify each over-ring and under-ring. Managers should sign off all voids and over-rings. Check signatures against those on file.

Limit the amount of accumulated cash in any register. Use a drop safe.

Check cash-to-sale ratios. These, along with unusually frequent refund transactions, can indicate employee theft.

Short-change artists frequently use large bills to pay...keep the tendered bills on the register until the transaction is concluded. Conduct only one transaction at a time. Do not be intimidated into rushing.

Counterfeit currency is difficult to detect. The look of the paper and its feel are usually the most obvious. Have your employees study characteristics of genuine bills so they will more readily recognize counterfeit ones (see following page).

# KNOW YOUR MONEY

## Design Features for Series 2004 Issued Currency

In 2004, the United States began issuing currency with a new multi-color design and additional security features. These elements were incorporated to increase the complexity of U.S. currency and attempt to thwart counterfeiting. Pre-existing security features such as the security thread, micro-printing, watermark, and optically-variable ink are included in the new notes and have only changed slightly.

### The New Design

The 2004 style of U.S. currency has the same historical figures and national symbols as the older series notes, in addition to having the same size and texture of the older bills. However, there are several new features that are unique to the 2004 style notes:

- A new offset-printed multi-colored background
- A slightly off-center borderless portrait
- An iconic symbol to the right of the portrait printed in metallic pigmented ink
- A new color-shift in the optically variable ink (OVI), from Copper to Green, when looking at the number in the lower right-hand corner of the bill when viewed from different angles
- The security thread is identical except for the \$50 bill where it is 50% wider and in a slightly different position.
- Micro-printing appears in different areas on each of the denominations.

Although all denominations of currency beginning with series 1996 have security features, the number of features will vary according to the note's denomination and series.



### Paper (Series 2004)

As with prior Series currency, the distinctive red and blue fibers are present beneath the colored ink in the background. As with 1996 style currency, each denomination bears a watermark depicting the same historical figure as the portrait, positioned to the right of the portrait beneath the multi-colored ink. In the \$10 bill, a hole in the multi-colored background permits easier viewing of the red and blue security fibers and the watermark.

If you doubt that a bill is genuine, ask the United States Secret Service, your bank or your local law enforcement agency.

**(Information on this page obtained from the United States Secret Service)**

## BANK DEPOSITS

If employees must carry deposits....



- ...vary the times.
- ...vary persons and use the “buddy system.”
- ...vary routes.
- ...leave the area if suspicious persons are present-complete your transaction later.
- ...place bank bags in indistinguishable bag or purse.

Contract for armored service, if possible.

Refer to “Robbery” section in this guide for further information.

## DOCUMENT HANDLING

Crimes against you or your customers could compromise your security or that of your customers or suppliers.

Shred all potentially sensitive materials including:

- customer lists.
- price lists.
- Prescription medicine receipts.
- invoices.
- applications for employment or credit
- customer output.
- documents with signatures.



Require that desks be cleared of important or confidential documents each night and that all file cabinets be locked when not in use.



## KEY CONTROL



1. Appoint a **key control officer** to manage the key and lock system.
2. Issue as few keys as possible. Keep **updated records** on the keys your issue.
3. Avoid the danger of key duplication. Caution employees not to leave keys with parking lot attendants, or in a topcoat hanging in a restaurant., or lying about in offices or stockrooms. Stamp keys “*Do not duplicate.*”
4. Have one key and lock for outside doors and a different key and lock for offices. **Do not have one “master key.”** Ask yourself if every employee really needs a key to every door.
5. **Code each key** so that it does not have to be visibly tagged. Do not use key chains with identifying tags.
6. **Lock keys** in cabinet or secured area.
7. **Recover** all issued keys upon separation.
8. Investigate loss of keys reported or discovered. **Re-key** affected locks, whenever a key is lost or an employee leaves the firm.
9. Consider installing locks that can be inexpensively recoded. A large variety of access control methods exist for your security needs.

## PROPERTY IDENTIFICATION

Engrave all company-owned items (office equipment, tools, machinery, etc.) with the owner's driver license number.

Property identification numbers can be affixed by engraving, etching, permanent adhesives, or by attaching microdots. Heavy equipment can be stamped or acid-etched. Bulk goods, such as hay or grain, can be identified with confetti on which the ID number is printed.

**TIP: CONTRACTORS:** Call the Construction Industry Crime Prevention Council for further information on loss prevention and recovery of heavy equipment.

## IF YOU SUSPECT THEFT....

Despite your best efforts, dishonest employees can find ways to beat the system.

If you suspect theft, do not "play detective" and try to solve the crimes. Make sure you do not jump to any unwarranted conclusions. False accusations could result in serious civil liability. Call your security consultants or the Sheriff's Department immediately.

## SHIPPING AND RECEIVING

Establish a **receiving procedure**, including where vendors are allowed to park and enter the business.

Do not permit trucks to dock until ready to load or unload.

**Check shipments** against bills of lading immediately to make sure all merchandise is there and that all merchandise is accounted for.

Shipping orders should be **controlled and numbered in sequence** to prevent padding or destruction.

Make a dependable **second check** of all incoming materials to rule out the possibility of collusive theft between drivers and employees who handle the receiving.

Do not permit drivers to load their own trucks, especially by taking goods from stock.

Consider **closed-circuit television** cameras on loading platforms. Locate monitors so they can be seen easily by employees and management.

Park company-owned on-site trucks and vans close together or against walls to prevent unauthorized access.



# CREDIT CARD AND CHECK FRAUD

Bad checks affect everyone in terms of higher consumer costs that must be paid to offset losses, as well as the cost involved in law enforcement and prosecution. Although it is only a minority that still uses checks, there is no fail-safe way to screen them, and even certified checks can be forged or altered. It is a business decision as to whether it should take the risk associated with check acceptance.

## AVOIDING BAD CHECKS

Set up a check-cashing and credit card acceptance policy to limit losses. Decide which checks you will accept and set a limit on the amount. The single most important element to cutting losses and providing customer service is **employee training**. Ensure that employees know and adhere to your policy. Here are some guidelines when establishing your policy:

### Never:

- ...take a postdated check or agree to hold a check for any reason.
- ...accept a check if the passer states he must make a deposit to cover it.
- ...be afraid to ask for good identification.
  1. The honest person doesn't mind.
  2. You may deter the dishonest.
- ...take a check from a person who is drunk or drinking to excess.
- ...let the person hurry you in your examination of a check or identification.
- ...accept a partial payment on a bad check if you contemplate legal action.
- ...accept a stale-dated check—usually six months is a maximum time that banks will accept a check for payment.
- ...accept an altered check or checks with erasures or written-over amounts.
- ...take double-endorsed (three-party) checks.



**Keep in mind:**

- Bad checks are most frequently passed on weekends and holidays.
- Out-of-state checks are hard to prosecute in California courts.
- Calling a telephone number on a check is not real protection against a forger.
  1. He may have an accomplice answer the phone number given.
  2. Anyone can get a name from the phone book.
- A bankbook is no proof of funds in the bank.
- A check is not legal tender (You are doing the customer a favor).
- A driver license or credit card alone is insufficient identification when cashing checks for strangers.
- Temporary licenses, social security cards, work permits, voter registration cards, and hunting or fishing licenses are NOT identification.
- Use a retro-reflective viewer to detect altered California licenses.
- You have no criminal recourse against the maker or payee on a two-party check.
- The police rely on merchants to report persons passing bad checks.
- The Sheriff's Department is not a collection agency.

**Always:**

- Limit staff cashing checks to one or two specially-trained members.
- Have the passer sign or endorse the check in your presence.
  1. If in doubt, reverse the check and have the endorser sign it on the other end.
  2. It may take time, but it saves money.
- Be sure that it is really a check, not a voucher or a merchandise order.
- Ask for good identification and compare both the description and the signature with that of the person presenting the check.
- Have your employees initial the checks at the time of acceptance.
- Examine every check to see that it is properly and completely made out. Call the bank if in doubt. Crooks do not usually go to stores that verify check information.
- If you call the Sheriff's Department, try to delay the subject without arousing suspicions.
- Try to get the subject's vehicle description and license number and direction of travel if he leaves before deputies arrive.
- Use care when dealing with "fast talkers" attempting to cash checks.

## REPORT TO LAW ENFORCEMENT

If you suspect forgery or a check proves to be fraudulent, notify security or law enforcement immediately. Obtaining goods with a bogus check and forgery are both felonies.

- Have the check in your possession.
- Be able to identify the check.
- Know who in your organization accepted the check.
- Provide a complete description of the suspect (can be written on the check).
- Report immediately after you are advised the check is not good.
  1. Law enforcement may have additional information.
  2. Lost time hinders a good investigation.

### Tips:

#### CHECKS

- Witness all endorsements.
- Are the local addresses and phone numbers correct?
- Is the date accurate?
- Are the location and branch of bank shown?
- Does the signature match with that on the ID?
- Are written and numerical amounts the same?

#### CREDIT CARDS

- Check the card number against the current "hot sheet" listings.
- Request valid photo ID.
- Compare signatures on the card and sales receipt.
- Check expiration date.
- Verify the card before approving purchase over the floor limit.
- Sales receipts must show only the last four digits of the credit card number.
- Contact store security and the card issuer if you suspect fraud.

## CURB CREDIT CARD CRIMES

Stolen credit cards can be reduced by alertness and proper security. Be aware of certain behaviors and clues such as:

- ...the chatty customer who delays a purchase until the clerk is upset, or the one who hurries a clerk just before closing.
- ...the customer who purchases without regard for price, size, color, style.

### Tell-tale signs of credit card fraud

- The card has been altered, has expired, or is not yet valid.
- Signatures on the card do not match.

### Remember

Do not accept credit cards without proof of identification.

# COMPUTER CRIMES

Computer crimes are defined as the illegal use of, or the unauthorized entry into a computer system or computer data to tamper interfere, damage, or manipulate the system or data. Computer crimes generally fall into one of the following categories:



- ▶ Unlawful access, destruction of or unauthorized entry into and use of computers systems, and the theft, interception, manipulation, destruction, or unauthorized disclosure of data stored within those computers.
- ▶ E-mail threats.
- ▶ Identity theft where technology is used to harvest data or produce counterfeit documents.
- ▶ White-collar crime, such as automated teller machine and credit card fraud, committed by means of electronic or computer-related media or networks.
- ▶ Theft of telecommunications service, theft, and resale of telephone calling codes, theft of wireless communication service, and theft of cable television services by manipulation of the equipment used to receive those services.
- ▶ Software piracy and other unlawful duplication of information.
- ▶ High-tech cargo theft, theft, and resale of computer components and other high technology products produced by the high technology industry.
- ▶ Remarking and counterfeiting of computer hardware and software.
- ▶ Theft of Trade Secrets.
- ▶ Crimes of violence or adult sexual exploitation where the victim and the perpetrator communicated on-line and such communications are relevant to motive, identity, or intent.

## **REDUCE VULNERABILITY**

To prevent damage from external events, the computer room and storage libraries must not be close to outside walls of a building. Interior walls need to extend to the true ceiling and should be reinforced.

- ▶ Restrict your business authorized personnel through a single entrance with other doors used as emergency exits only.
- ▶ Protect computer information as you would any valuable corporate asset.
- ▶ Control administrative rights to the computer.
- ▶ Stay informed about new security devices and information.

Classify information into categories based on importance and confidentiality to your business, such as "confidential" and "sensitive." Identify software, programs, trade secrets, and data files that need special protection. Use non disclosure and non competitive contracts.

Define **Acceptable Use Policies** which establish clear employee guidelines for standards of conduct relating to computer use, including removal of disks, remote access, Internet usage, personal us, secure passwords or printed output.

## **PROTECT YOUR COMPUTER FROM INFECTION**

- ▶ Don't bring diskettes in from outside sources or any removable drives (i.e. USB Thumb Drives) unless you are absolutely sure of the data contained on the disk or drive.
- ▶ Use an Anti-Virus Program that includes malware and spyware protection and a software firewall.
- ▶ Use a hardware firewall with an intrusion detection system.



## COMPUTER VIRUSES

A computer virus is a computer program that causes intended, annoying, or destructive results. Some are relatively harmless, while others may destroy valuable data. Some common examples are:

- ▶ Trojan horses
- ▶ Logic bombs
- ▶ Trap doors
- ▶ Worms, etc
- ▶ Malware can be used to steal passwords or sensitive information and take over control of your computer.
- ▶ Spyware is used to track your movements on the Internet.



Reduce chances of virus access by:

- ▶ Scanning demo disks from vendors, shareware, or freeware sources for viruses on a computer which is not networked and has up to date virus protection, malware and spyware software installed.
- ▶ Scanning downloaded files for virus infection. Avoid downloading executable files.
- ▶ Making regular back-ups to aid in recovery.

It is your responsibility to ensure that customers' and clients' personal information is protected. There are several measures that can be used to reduce the risk of unwanted access to computer files.

- ▶ Implement detective controls.
- ▶ Design audit trails into your computer applications.
- ▶ Log all access to computer resources with unique user identification. Ensure that logging is turned on for all of your servers including but not limited to email servers, file servers, network servers, and routers.
- ▶ Change administrative rights passwords to make them secure. (Do not use the default passwords). Separate the duties of systems programmers, application programmers, and computer programmers.
- ▶ Encrypt confidential data stored in computers
- ▶ or transmitted over communication networks using National Institute of Standards and Technology (NIST) data encryption standards.
- ▶ Establish clear procedures for recovering your data from accidental or unauthorized destruction.
- ▶ Routinely back up all of you computer systems keeping a copy on site and a copy off-site at a secure location.

## DETECT PROBLEMS.

**Monitor** activities of employees in positions of trust who handle sensitive or confidential data. **Watch** for employees who work abnormally long hours or who refuse to take time off as many computer crime schemes require regular, periodic perpetrator manipulation to avoid detection. **Be aware** of employees who collect material not necessary to their jobs, such as programming manuals, printouts for data and programs and software manuals. Review data files periodically for irregularities.

Review automated audit information and control reports to determine if there have been repeated, unsuccessful attempts to logon, both from within and outside your facility. Look for unauthorized changes to programs and data. When employees are terminated voluntarily or involuntarily restrict access immediately.

**High-tech crimes are often time-sensitive.** Frequently the information you need to identify a perpetrator must be tracked down immediately or lost forever. Internet service providers frequently erase their logs after just a few days or weeks. Contact local law enforcement immediately.

# ARSON

Arson is one of the most expensive crimes against businesses, sometimes forcing a firm to close shop, causing the loss of jobs as well as loss of tax income to the community.

The crime of arson is difficult to prove since the perpetrator is rarely seen in the act of setting the fire.



## Some arson motives:

- Profit
- Revenge
- Social interest
- Pyromania
- Boredom

## PREVENTION

Secure all doors, windows, skylights and gates as well as storage areas.

Educate your employees about the facts of arson and fire safety.

Install automatic and tamper-proof sprinklers.

Secure flammables in a locked, fire-resistant cabinet. Dispose of all flammable waste materials promptly.

Establish frequent, regular fire drills and maintain an up-to-date emergency plan.

Report suspicious actions and any information which might aid law enforcement.

### SAFETY TIP

Make sure your smoke detector batteries are fresh. Change them twice a year when you change your clocks.

Check the fire extinguishers annually.

Properly dispose of all flammable waste materials.



# PERSONAL SECURITY

Security precautions should not create additional hazards for facility occupants. For example, barrier devices should not interfere with the ability of building occupants to leave quickly in the event of fire or other emergency.

Security enhancement can be as simple as insisting that employees lock up purses and other belongings or encouraging employees to protect their vehicles from theft and burglary.



## ASSAULT PREVENTION

Burglars, robbers, and thieves seek primarily to remove cash or property. Nevertheless, many such intruders are capable of harming people with little provocation. In general, facility occupants should be trained to avoid confrontation with the criminal. Instead, they should report the incident as soon as they feel it is safe to do so.

The “buddy system” (safety-in-numbers concept) is recommended for the following vulnerable times:

- **Opening the business**--If possible, schedule two employees to meet and unlock the business together. One should stay outside, while the other checks the interior. After assuring that all is clear, they may enter the building.
- **Closing the business**--Employees should have partners accompanying them to their vehicles, especially at night. If this is not possible, request that a security guard for the shopping center escort the last employee to his or her car.
- **Bank deposits**—Making bank deposits alone can be dangerous. If employees must make deposits, they should go in pairs. If you are alone, vary deposit times and carry the deposit inside a purse or bag other than a shop-named bag or bank bag. Deposits should not be made after closing by a lone employee who just closed the shop. This is an ideal time for a robbery!
- **Taking out the trash**—Doing this in pairs is much safer, both for the employees and for the business.

*Controlling access enhances personal security.*

- Keep secondary exits locked, but still in accordance with local fire codes. Limit secondary exits by non-employees (this includes ex-employees) by having the doors alarmed and labeled “EMERGENCY EXIT ONLY!”, or by limiting access to the area around the door.

- **Keep restrooms locked.** Be in control of access to restrooms, storage areas, etc. This prevents assailants from hiding in waiting and “breakouts.”
- In many businesses, ID badges can be used for access control. They are, however, only as effective as the enforcement of the ID policy.
- Install a panic button at the front counter. Make sure there are phones near both front and rear entrances.

*Visibility increases safety.*

- Keep parking and walking areas well-lit. A good standard by which to gauge lighting is to provide at least one foot-candle of light everywhere in the parking lot and around the perimeter of the building.



- Keep the area around your building clear of debris and accumulated materials. Stacks of pallets and boxes can be hiding places for assailants.
- Install mirrors or CCTV in rooms with “blind corners” and in enclosed parking facilities.

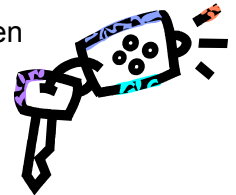


**TIP:**

It is usually more cost-effective to replace all light bulbs at once than to replace bulbs as they burn out. When bulbs are replaced, lenses should be cleaned.

*Keeping employees aware helps keep them safe.* Employees should:

- Keep the building locked whenever public access isn't necessary (after closing, in an office, etc.).
- Have keys in hand when leaving the building.
- Watch for suspicious persons (anyone who does not seem to have legitimate business with you).
- Look in your car before entering.
- If you think you are being followed, go into an open business or find other people.
- Use the “buddy system.”
- Take access control policies seriously.



*If a confrontation does occur, remember these personal safety procedures:*

- **Don't be a hero.** Do nothing to risk your personal safety.
- Consider all guns or threats of guns as loaded weapons.
- **Activate alarms** *only if you can do so without detection.*
- Attempt to alert coworkers if you can do so safely.
- **Follow directions** exactly, without volunteering.
- Without seeming obvious, *study and memorize* attacker's distinguishing features.

# BUSINESS WATCH

**Business Watch** is a program organizing business people to work with local law enforcement officers to reduce crime. Similar in concept to the residential Neighborhood Watch Program, the basic goals are threefold:

- Reduce crimes affecting businesses.
- Provide enhanced inter-business communication.
- Increase the criminals' risk of apprehension.

Services offered include:

- Personalized Commercial Security Consultations at no charge.
- Training about how to use an engraver to mark business property.
- Training programs about robbery prevention, shoplifting, fraud, and internal theft.
- Availability of recognized warning signs, stickers and decals.
- Crime reporting workshops.
- Crime Information Network assistance.



To keep the benefits of Business Watch cost-effective, every effort is made to schedule meetings without intruding on production time. The program offers great flexibility: Business Watch is tailored to meet the specific needs of your community or your industry.

Establishing a Business Watch is free through the Sheriff's Department. Most of the materials are provided by the Crime Prevention Unit. Aluminum Business Watch signs and decals are available for your group to purchase through outside vendors.

If you are interested in starting a Business Watch Program, contact your local Crime Prevention Unit.



# ROOFTOP NUMBERS

Many times, law enforcement uses aerial support to apprehend a fleeing suspect. In order to help identify the area of focus for the helicopter, the Sheriff's Department recommends that businesses paint their address numbers on their roofs. There are certain dimensions that should be used in order that the numbers are effective.

## MINIMUM REQUIREMENTS

- Height: 36" \*Lines should be 4-6" wide\*
- Color: For most roofs, a reflective white contracts best. If the rooftop is white or light, contrast with black.
- Lettering: Should include the full street number. The street name is not necessary.



➤ Numbers can be painted, using a high-quality exterior paint. Plastic U.V. coated numbers are available through commercial supply vendors.

➤ Numbers may be placed on the front or rear of the roof area, as long as it can be clearly viewed. If your roof pitches toward the street, you may wish to place the numbers on the back side of the roof.

## Special Recommendations

SCHOOLS: Name of the school should be on the roof. Street numbers, optional.

COMMERCIAL: First letter of each word, plus numbers  
(example: SDCU 13556 for San Diego County Credit Union)

RESIDENTIAL: 24" height, numbers only. Recommend one address on a roof for every block.

5693

# BOMB THREATS

Develop a policy for reporting all crimes. Place emergency telephone number stickers with your business name, address, and phone number on all phones. Have a specific plan for reporting and evacuating in the event of a bomb threat. Designate two different areas outside the buildings for employees to congregate. Make your evacuation plan a routine part of orientation. Clip and copy the checklist reproduced here and place copies throughout your office.

## IF A BOMB THREAT IS RECEIVED....

1. **Be calm and courteous.** Do **not** interrupt the caller.
2. If possible, **notify someone** else by a prearranged signal to listen in on the conversation while the caller is on the line.
3. Keep the caller on the line as long as possible. Ask him/her to repeat the message. **Record** every word spoken by the caller. Ask the caller his/her name and why he/she is doing this. There is a chance he will reveal it.
4. **Inform** the caller that the detonation of a bomb could result in death or serious injury to many *innocent* people.
5. Pay particular attention to peculiar **background noises**, such as motors running, background music, and any other sounds that may give indication about the location of the caller.
6. Listen closely to the **voice** (male, female), **voice quality** (calm, excited) **accents**, and **speech impediments**. Immediately after the caller hangs up, complete the *Bomb Threat Checklist* and report to the person designated by management to receive such information.
7. **Report** bomb threats immediately. Law enforcement personnel will want to talk firsthand with the person who received the call. That person should remain available until officers arrive.

## BOMB THREAT CHECKLIST

Exact time of call: \_\_\_\_\_

Exact words of caller: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Questions to ask:

1. When is the bomb going to explode? \_\_\_\_\_

2. Where is the bomb? \_\_\_\_\_

3. What does it look like? \_\_\_\_\_

4. What kind of bomb is it? \_\_\_\_\_

5. What will trigger the bomb? \_\_\_\_\_

6. Did you place the bomb? \_\_\_\_\_

7. Why? \_\_\_\_\_

8. Where are you calling from? \_\_\_\_\_

9. What is your address? \_\_\_\_\_

10. What is your name? \_\_\_\_\_

**CALLER'S VOICE** (circle):

calm	disguised	nasal	angry	broken
stutter	slow	sincere	normal	rapid
giggling	deep	crying	squeaky	loud
stressed	accent	excited	slurred	lisp

If the voice is familiar, who did he/she sound like? \_\_\_\_\_  
\_\_\_\_\_

Were there any background noises? \_\_\_\_\_

Remarks: \_\_\_\_\_  
\_\_\_\_\_

Person receiving the call \_\_\_\_\_

Telephone number call received at \_\_\_\_\_

Date \_\_\_\_\_

**Report incident immediately to law enforcement (9-1-1)**