VICTORIA POLICE

BUSINESS SECURITY
INFORMATION KIT

AGGRESSIVE **PEOPLE**

As a business owner / operator you have a responsibility to maintain a safe working environment for all employees and customers. Your safety, and the safety of others, comes first. Violence can be prevented or minimised through sound risk management strategies and good communication.

Violence can occur when:

- Employees confront people stealing;
- Troublemakers create conflict because they're bored, showing off, or distraction tactics while someone else is engaged in an unlawful act;
- Customers dispute or complain about goods and services, including requesting refunds, anger over long waits in queues, etc;
- Employees are managing people suffering mental illness or who appear to be affected by alcohol or drugs.

These types of events can result in violent behaviour consisting of:

- Verbal abuse, such as offensive remarks, swearing or name calling;
- Actively hostile behaviour, including shouting, fist shaking or threatening gestures;
- Physical abuse that may result in injury or damage.

While the vast majority of customers are polite and friendly to deal with, violent outburst that occur inside a store or small business can result in physical injury to employees, customers, or the offender and damage stock or fixtures. It may be useful to keep copies of the Description Form (**Appendix A**) in a convenient location within the business for quick and easy reference and use by employees to assist the police in a later investigation of the matter.

PREVENTION

Training employees in good customer service and educating them about conflict resolution can be a useful investment in avoiding customer complaints and potential risks such as those outlined above.

Arrange floor fit outs to have wide counter areas to act as a natural barrier between employees and aggressive customers. Ensure employees have escape corridors from these areas as well.

Security measures such as duress or panic alarms and access controls to employee areas should be considered. Emergency contact details should be located near all telephones and all employees should know the procedures to be used in the event of encountering an aggressive person.

BASIC TIPS TO DIFFUSE A SITUATION

- Assess the situation and remain calm and non-confrontational;
- Stay Safe;
- Keep a safe distance, use natural barriers such as counters etc;
- Talk calmly, don't raise your voice to match the aggressors;
- Do not respond to the aggressor's bad behaviour with bad behaviour yourself;
- If the business employs security personnel employees ensure they are informed and attend;
- Allow the aggressor to vent his anger with minimal interruption;
- Remain respectful. Be empathetic to the aggressors' problem/s. Explain what options are available and encourage them to try one of them;
- Patience is usually a good strategy and this can be achieved by not only listening to the person but by acknowledging their problem or situation:
  - Employees should not take insults personally;
  - Anger will diminish over time;
  - If the person is suffering from a psychotic episode then their connection with reality usually rises and falls over time.
- Other employees not involved in the incident should not become an audience; however they should monitor the situation for any possible escalation;
- If the person is not able to be calmed and they continue to be offensive or obnoxious, politely request the person to leave the store;
- After having been politely requested to leave the store, a person refuses, contact the police on **Triple Zero (000)** and await their arrival. Do not engage in any further unnecessary dialogue.

VIOLENT OFFENDERS

- Do not enter the person's physical space as this can escalate the situation. Holding your stance can appear aggressive to the offender - consider stepping back etc;
- Discreetly remove any items that could potentially be used as weapons;
- Counter areas or display stands can be discreetly used to create natural barriers and distance between employees and the other person;
- Employees are entitled to protect themselves from violence if they believe their conduct is necessary in self-defence; and their conduct is a reasonable response in the circumstances, as the person perceives it. The amount of force used to deter violence, must be reasonable and proportionate to the harm that is being avoided. Excessive force is not justified and can result in a counter-claim of criminal assault or civil litigation.

If the situation is becoming out of control and the safety of employees or customers is at risk, contact police immediately on **Triple Zero (000).**

POST EVENT ASSISTANCE

The Victims Support Agency (VSA), within the Department of Justice and Regulation, is the official Victorian Government agency helping people manage the effects of violent crime.

VSA represents people affected by crime, coordinating a whole-of-government approach to services for victims. The agency operates the Victims of Crime Helpline, and funds state-wide services to provide victims with practical assistance, counselling and support through the justice system.

VSA is pivotal in linking victims to service systems, ensuring they receive personalised, timely and effective support to manage the effects of violent crime.

Further information is available at victimsofcrime.vic.gov.au

FURTHER INFORMATION

Further information to assist your business is available from the following sites:

Victoria Police Crime Prevention

police.vic.gov.au/communitysafety

Work Safe Victoria

worksafe.vic.gov.au/safety

Australian Institute of Criminology

aic.gov.au

Victims Support Agency

victimsofcrime.vic.gov.au

Victims of Crime Commissioner (VoCC)

victimsofcrimecommissioner.vic.gov.au

ARMED **ROBBERY**

Under Australian Workplace Safety legislation all businesses have a legal duty to provide a safe workplace, so they need to be thoroughly prepared for the possibility of an armed robbery on their premises.

Planning may assist in reducing the risks of armed robbery to your business, thereby maximising the safety of your employees and customers.

The aim of any planning around armed robberies should be to:

- Prevent the business being targeted by offenders;
- Increase the safety of employees and customers;
- Reduce the impact of the crime on the business;
- Assist police in the arrest of any offender/s.

PREVENTION

1. Good visibility

Maintain a workplace that is highly visible from the street. An open, uncluttered environment providing a clear, well-lit view of the sales area can deter offenders. Do this by ensuring advertising material, posters and curtains are kept to a minimum, so as to provide a clear view of the premises from both inside and outside. Ensure there is strong bright lighting both internally and externally.

2. Alertness

Be alert to strangers or individuals who may be observing the business, or who are asking operational questions about how the business runs. Individuals whose actions are out of character, such as winter clothing on a summer day, motor bike helmets or dark sunglasses inside businesses should be monitored.

3. Lock doors

Ensure all back doors, side doors, windows and store rooms are secured with deadlocks, key locks and / or bars. These points should be kept secured at all times.

4. Safes

Do not discuss cash holdings or movements of cash in public. Install time delays on all safes; install drop safes and chutes so the contents cannot be accessed by employees. This can minimise the amount of money stolen and provide employees with a valid reason to only hand over visible cash. This also prevents periods when the safe has to be opened for employees to deposit cash. Where possible do not handle or move cash in the presence of the public. Encourage the use of electronic fund transfers for payments and wages.

5. Secure Areas

Sales areas should only be used by employees and be monitored and secured at all times. Install barriers to keep people out of these areas. The counter or work area should be wide and elevated to provide visibility and safety for employees. Secure cash registers to the counters.

6. Security Devices

Install good quality CCTV (Closed Circuit Television), have monitored alarms, sensors or alarms that alert employees to customers entering or leaving and duress / panic type alarms. Make use of signage to advise potential offenders of the high security measures utilised at the premises, in an effort to discourage them from attempting unlawful acts.

7. Training

Ensure all employees are provided with information, instruction training and supervision to ensure security procedures are relevant and applied in practice. Employees should be consulted in the development of procedures and be given the opportunity to provide feedback on potential improvements. A list of relevant telephone contact numbers should be readily accessible in the event of an emergency situation.

8. Avoid Predictability

Don't establish a routine that makes cash handling procedures predictable. Vary banking times where possible; avoid cash counts at close of business. If large amounts of cash are to be moved, consider using professional security companies.

9. National Name Checks

Consider conducting a National Name Check (Police Check) on all employees at the time of recruitment. National Police Record Check - Victoria Police provides a service to all Victorians who wish to obtain a National Police Certificate for employment, voluntary work and occupation-related licensing or registration purposes.

Information about an individual's criminal history will not be released without an applicant's written consent other than for law enforcement purposes - go to police.vic.gov.au/policecheck for further information.

DURING AN ARMED ROBBERY

1. During an armed robbery the most important thing to do is **stay safe**;
2. Try to remain calm, assess the situation and do exactly as the offender says. Remember the number one priority is your safety, the safety of other employees and customers;
3. Activate alarm devices as soon as possible, but only if it is safe to do so;
4. Obey instructions, but do not provide any cash or goods that are not asked for. Advise the offender of any movements you have to make to comply with his / her instructions. Do not make any sudden or unexpected movements;

5. Speak only when spoken to as any conversation with the offender will prolong the incident;
6. Don't attempt to retaliate or attack the offender;
7. Avoid eye contact with the offender and show your hands;
8. Where possible, try to make mental notes of the offender and the situation including height, hair colour, scars, tattoos, accent and speech. Also note the description of the offenders clothing and descriptions of any weapons used;
9. If safe to do so, look to see if a vehicle has been used and if there are any other occupants, record the registration number, make, model and the colour of the vehicle;
10. Never take drastic action during the robbery and do not chase the offenders.

AFTER THE ROBBERY

1. Immediately contact police on **Triple Zero (000)**, even if you have activated a hold up or duress alarm. Tell the police telephone operator:

- If anyone has been hurt at the scene;
- That an armed robbery has occurred;
- Exact location including the business name and address of where the crime occurred and the closest intersecting street;
- Your name, address and contact phone number;
- Date / time / nature of offence;
- Number and description of offenders including any vehicles used;
- Direction of travel;
- Whether any weapons were seen / used and what type they were.

2. Only hang up the telephone when told to do so and stay off the phone until police arrive unless you remember additional information that may be important.
3. Close the premises to the public and keep unauthorised persons out.
4. Make sure no person touches or moves any items where the offender/s was / were present.
5. Consider arranging someone to meet police outside, particularly in large shopping areas to make the response time more efficient.
6. Request that witnesses and customers remain until police arrive - failing that, request their names, addresses and telephone numbers and pass them onto police when they arrive.
7. Make sure witnesses are isolated from each other or are aware not to discuss the descriptions or what happened with other witnesses.
8. Witnesses should independently try to write, in as much detail as possible, a description of offender/s and what occurred. This could be by way of completing an Offender Description Form (**Appendix A**) that should be located in a convenient place accessible by employees. These should then be handed to police when they speak with the witness.
9. Do not make any statements to the media before discussing the matter with police.
10. Supply police with all details no matter how insignificant they appear to you. This could include earlier suspicious customers, rude, drunk or drug affected customers, upset former employees or simply details of certain cars constantly driving past.
11. Crime affects different people in different ways and the impact may not be felt immediately. Consideration should be given to organising professional trauma counselling for employees affected by the crime.

POST EVENT ASSISTANCE

The Victims Support Agency (VSA), within the Department of Justice and Regulation, is the official Victorian Government agency helping people manage the effects of violent crime.

VSA represents people affected by crime, coordinating a whole-of-government approach to services for victims. The agency operates the Victims of Crime Helpline, and funds state-wide services to provide victims with practical assistance, counselling and support through the justice system.

VSA is pivotal in linking victims to services, ensuring they receive personalised, timely and effective support to manage the effects of violent crime.

Further information is available at victimsofcrime.vic.gov.au

FURTHER INFORMATION

Further information to assist your business is available from the following sites:

Victoria Police Name Checks
police.vic.gov.au/policecheck

Victoria Police Crime Prevention
police.vic.gov.au/communitysafety

Work Safe Victoria
worksafe.vic.gov.au/safety

Safe Work Australia
safeworkaustralia.gov.au

Australian Institute of Criminology
aic.gov.au

Victims Support Agency
victimsofcrime.vic.gov.au

Victims of Crime Commissioner (VoCC)
victimsofcrimecommissioner.vic.gov.au

CASH HANDLING

The safe handling of cash within a business environment can assist in preventing crime. Cash handling incorporates not only general cash security, but also the secure storage and transport of cash.

Having procedures and control measures in place that all employees are familiar with and comply with, will greatly reduce the risk of cash robberies and injury to employees. Employees should be familiar with and trained in the use of the equipment they are required to use, and the procedures and control measures to be utilised to minimise robberies. These include:

- Operating security devices and alarms;
- Communication systems;
- Staffing levels;
- Cash limits;
- Planning and changing transport routes / times to minimise predictability;
- Confidentially about procedures and security devices;
- Situational awareness and how to identify suspicious behaviour;
- Emergency plans and procedures including how to respond during and after a robbery or violent incident;
- Support after an incident.

CONSIDERATIONS RELATING TO CASH ON PREMISES

Environmental crime prevention interventions include, but are not limited to, activities such as improved security through strengthening locks, improving surveillance, improving street lighting, installing closed circuit television, putting locks on windows, introducing safer money handling procedures, and limiting the amount of money held on the premises.

1. Money stored as a float on the premises should be kept to a minimum;
2. Individual floats should be kept as small as possible;
3. Advertise that only a minimum amount of cash is kept on the premises;
4. To minimise damage to cash registers by after-hours thieves, leave your tills empty and open overnight. This will avoid an offender damaging the cash register to find out there is nothing inside;
5. Consider installing a safe that is securely fitted to a solid object;
6. Safe keys and combinations should be stored securely and separately;
7. Ensure that before cash is counted, the attending employee is in a safe and secure area of the business that is out of public view. This may include checking the premises, including the toilets and other concealment locations such as large cupboards, for people who may be hidden;
8. A policy limiting entry into premises or requests for exact change at night, prevents customers seeing cash holdings;
9. Make sure all exterior doors and windows are properly secured from the inside before counting money;
10. If cash is being counted in a specific area, consider installation of a telephone, duress (panic button) alarm system or CCTV at your site;
11. Don't discuss cash amounts or handling procedures in public;
12. It is not advisable to take cash home and be known to do so;
13. If employees are utilised to courier deposits, it is recommended that they be criminal and reference checked, suitable and able bodied, properly trained in cash carriage procedures and robbery response, be comfortable with the duty and have access to a mobile telephone. A National Police Check can be utilised to conduct a check on employees and further information can be located at police.vic.gov.au/policecheck

TRANSPORTING CASH IN-HOUSE

The most effective way to eliminate or minimise risks to you and your employees, so far is reasonably practicable, is to engage a professional security company to transport cash. You should consider this option first. Consider using a security transport company when:

- Cash needs to be transported often;
- Large amounts of cash are involved;
- Cash is transported long distances, and;
- The area where the cash is transported has a high crime rate.

If you use a security transport company you should work closely with the security company to assess risks and implement suitable control measures.

Consider varying cash collection times and introducing a system to confirm the identity of the security guard/s. Their identification card should always be presented and checked. Advise employees that guards should be wearing the uniform of the security company. If they are suspicious of the guard they should not directly confront the guard, but alert police and your security company as soon as possible. Police should be contacted on **Triple Zero (000)** if suspicious.

WALKING ROUTES

Moving cash from a workplace to a bank exposes workers to the risk of robbery.

Where it is not reasonably practicable to use a security service to transport cash, use a bank close to the business to deposit takings. Change the procedures for transferring cash often, including routes, times, schedules, the amounts transferred and the vehicle used for the transfer. Avoid banking alone; rotate the task so it is not always the same person visiting the bank.

- Vary the route and time of day when the person goes to the bank so movements cannot be predicted;
- Avoid using quiet streets and alleyways;

- Only make the journey when other people will be around;
- Use a busy route and walk in the centre of the pavement facing oncoming traffic;
- Identify vulnerable spots along the route and maintain extra vigilance in those areas;
- Check the area outside the premises before leaving the premises or bank. Be aware of any suspicious people and / or vehicles around the workplace;
- Be observant for any suspicious behaviour and report any behaviour that causes concern immediately to police on **Triple Zero (000)** with a description of the person or vehicles arousing suspicion.

MODE OF TRANSPORT

Where possible, travel by motor vehicle rather than on foot or using public transport. Use vehicles in good mechanical condition and appearance and where possible have no distinguishing features. Try not to use the same vehicle each time.

APPEARANCE

- Wear plain clothing rather than a uniform to be less conspicuous;
- Do not take large amounts of cash to the bank, in the same bag, at the same time every day;
- Use security bags, unmarked bags or containers to carry cash and do not draw attention to them;
- Use cash carrying waistcoats so it does not look like cash is being carried.

COMMUNICATION AND TRAINING

- Ensure workers are trained and understand what precautions they should take when they are transporting cash;
- Tell the bank the expected arrival time and another employee the expected return time.

POST ROBBERY PROCEDURES

An armed hold up or other violent incident is dangerous and frightening for workers. Post hold up procedures should be set out in your emergency plan and include:

- Calling emergency services - as soon as it is safe to do so contact police and if necessary an ambulance, via **Triple Zero (000)**;
- Providing first aid - injured or traumatised workers and members of the public should be given first aid;
- Assisting the police - workers should be given guidance on what they can expect from contact with police after the incident e.g. leaving evidence undisturbed and reporting what and who they saw;
- Contacting victims' families and other workers;
- Providing and encouraging counselling for workers involved and workers affected by the incident i.e. colleagues of the victim/s;
- As part of the recovery process, provide debriefings to workers to share information about the incident;
- Reviewing risk assessments and control measures.

The short and long term psychological effects of being confronted with violence can be severe and debilitating. It is important not to judge or criticise a person's behaviour during a holdup and not to trivialise the event or be unsympathetic.

Workers should be given the opportunity to receive follow up post trauma counselling and other suitable support. Consider providing in house or external post-traumatic stress counselling from psychiatrists or psychologists who are experienced in post trauma debriefings and counselling.

Contact workers who take time off after an incident to check they are receiving suitable medical and psychological help.

Consider offering workers the opportunity to return to work in another role, or at another site if they are too traumatised to resume their previous role.

POST EVENT ASSISTANCE

The Victims Support Agency (VSA), within the Department of Justice and Regulation, is the official Victorian Government agency helping people in Victoria manage the effects of violent crime.

VSA represents people affected by crime, coordinating a whole-of-government approach to services for victims. The agency operates the Victims of Crime Helpline, and funds state-wide services to provide victims with practical assistance, counselling and support through the justice system.

VSA is pivotal in linking victims to service systems, ensuring they receive personalised, timely and effective support to manage the effects of violent crime.

Further information is available at victimsofcrime.vic.gov.au

FURTHER INFORMATION

Further information to assist your business is available from the following sites:

Victoria Police Name Checks
police.vic.gov.au/policecheck

Victoria Police Crime Prevention
police.vic.gov.au/communitysafety

Work Safe Victoria
worksafe.vic.gov.au

Safe Work Australia
safeworkaustralia.gov.au

Australian Institute of Criminology
aic.gov.au

Victims Support Agency
victimsofcrime.vic.gov.au

Victims of Crime Commissioner (VoCC)
victimsofcrimecommissioner.vic.gov.au

Crime Statistics Agency Victoria
crimestatistics.vic.gov.au

CCTV

Closed Circuit Television, otherwise known as CCTV, is a type of video monitoring system, which has been around since the 1940s. CCTV systems are based on strategically placed video cameras, which capture footage and then broadcast it to either a private (closed) network of monitors for real time viewing, or to a video recorder (either analogue or digital) for later reference.

It has become an increasingly important factor in security and surveillance for governments, law enforcement, schools, businesses and home owners.

A CCTV system is not a physical barrier and does not limit access to certain areas, make an object harder to steal or a person more difficult to assault and rob, but it does have some crime prevention capacity in the right situations. Although CCTV has many functions, the primary preventative utility is to trigger a perceptual mechanism in a potential offender. It seeks to change offender perception so the offender believes if they commit a crime, they will be caught. In other words, CCTV aims to increase the perceived risk of capture, a factor which, assuming the offender is behaving in a rational (or limited rational) manner, will de-motivate the potential offender/s. For this crime prevention process to succeed, two elements must exit:

- The offender must be aware of the cameras' presence; and
- The offender must believe the cameras present enough risk of capture to negate the rewards of the intended crime.

LAWS REGULATING CCTV

The use of CCTV cameras in Victoria is governed primarily by the *Surveillance Devices Act 1999* (Victorian Legislation). The *Privacy Act 1988* (Australian Federal Government Legislation) should also be used as a reference when considering CCTV use, in particular the displaying of images.

In short, you cannot use an optical surveillance device to view or record a private activity without a warrant. Whether the place is a public place or a private place, or public or private property, is not relevant in Victoria.

In the case of CCTV, these devices need to be set up so they do not view or record a private activity. A private activity is defined as an activity carried out in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves, but does not include -

- An activity carried on outside a building or;
- An activity carried on in any circumstances in which the parties to it ought reasonably expect that it may be observed by someone else.

Circumstances in which parties to an activity ought reasonably expect that they may be observed by someone else include:

- Activities in places accessible to the public;
- Activities in those parts of the workplace accessible to other employees or invitees of that workplace.

Circumstances in which parties to an activity may reasonably expect that they may not be observed by someone else include:

- Activities in toilet cubicles and shower areas;
- Activities in change rooms;
- Activities in those parts of the workplace where the parties to the activity may exclude others from observing the activity, such as in an office with covered windows.

Contrary to popular belief, there is no law that prevents a person taking photographs or filming another person without that person's consent.

Using cameras on private or public property is legal provided the owner does not object and you are not filming in a way which is meant to record people when they ought to reasonably believe they were entitled to privacy.

The use of voice / sound recording in conjunction with CCTV is primarily regulated by the same Act. Basically, if the person recording the conversation is not part of the conversation then the conversation cannot be recorded without the authority of a warrant and these will not be issued to persons or businesses, as they are essentially for law enforcement use only.

In Victoria there is no requirement to display signage advising people that video surveillance is operating, but the use of signage makes the potential offender more aware of the existence of CCTV surveillance which may deter them.

WHERE TO USE CCTV

- After hours surveillance of areas that have little or no natural surveillance from passing motorists, pedestrians or employees;
- Areas at risk to vandalism, graffiti, theft or other criminal offences;
- High risk areas such as computer rooms or cash handling areas that are not adequately protected by employee surveillance;
- Entrances, exits, front counter areas etc.

EQUIPMENT CONSIDERATION

There is a wide range of CCTV equipment available. Pricing increases with the quality of the product and the product it delivers.

Obtaining the advice of a competent person or company in the CCTV surveillance field may save a lot of frustration and expense. These people / companies can be found on the internet and in local publications.

There are two types of CCTV systems: digital and analogue. In the past, analogue technology and video surveillance (recorded in the moment activity onto video tape for future access) was the only option. However, since it does not broadcast actual live information, analogue is not practical for monitoring stores from a remote location. The picture quality is low and often unusable, and relied on human intervention as well, such as changing the tapes regularly. Digital CCTV is revolutionising security measures and technology has evolved to allow for a more diverse security monitoring system.

A contributing factor on deciding which technology to adapt for your premises is if the location has previously been cabled for CCTV or not. In short, if it will be a 'new' install then IP/Digital system with network cable is the best option. If it is an upgrade from analogue coaxial cable system, technology now exists to upgrade to High Definition using the existing cable. A security adviser/ installer can assist you with the decision.

CAMERAS

When building a surveillance system, it is important to select cameras that meet the needs of your business and installation. This includes selecting specific types of cameras to meet the intricacies of the venue location. For example, retail environments will have different needs than schools or outdoor facilities, and every installation has some features that are more important than others.

Dome CCTV camera - Dome CCTV cameras are most commonly used for indoor security and surveillance applications and get their name from the dome-shaped housing in which they sit. These housings are designed to make the CCTV cameras unobtrusive and not covert or hidden. Typical applications are for retail premises, where the camera is designed to be unobtrusive, but visible. The "dome" shape makes it difficult to tell the direction that these cameras are facing, and thus are ideal for deterring criminals. Potential offenders will know the facility is being watched and customers will feel at ease knowing the facility is being protected. Units that allow the camera to pan / tilt / zoom and spin quickly within the housing are often referred to as 'speed domes.'

Bullet CCTV camera - Bullet CCTV cameras have a long, cylindrical, and tapered shape, similar to that of a 'rifle bullet', often used in applications that require long distance viewing. The camera is not typically designed to have pan / tilt / zoom control but instead to capture images from a fixed location, pointing at a particular area. A bullet CCTV camera is a wall or ceiling mounted unit that is typically designed for indoor use, but can also be used for some outdoor applications. Many bullet cameras can also be waterproofed by being installed inside protective casings, which protect against dust, dirt, rain, hail and other harmful elements.

C-Mount CCTV camera - C-Mount CCTV cameras have detachable lenses to fit different applications. Standard CCTV camera lenses can only cover distances of between 10 and 12 metres, therefore with C-Mount CCTV cameras, it is possible to use special lenses which can cover distances greater than 12 metres.

Day / Night CCTV camera - Day / night CCTV cameras have the distinct advantage of operating in both normal and poorly-lit environments. These cameras do not have infrared illuminators because they can capture clear video images in varying light conditions and in the dark. The camera is ideal for outdoor surveillance applications, where infrared CCTV cameras cannot function optimally. These CCTV cameras are primarily used in outdoor applications and can have a wide dynamic range to function in glare, direct sunlight, reflections and strong back light 24/7.

Infrared / Night Vision CCTV camera - These night-vision CCTV cameras have the ability to see images in pitch black conditions using infrared LEDs and are ideal in outside conditions where lighting is poor to zero.

Network / IP CCTV camera - These cameras, both hardwired and wireless, transmit images over the Internet, often compressing the bandwidth so as not to overwhelm the web. IP cameras are easier to install than analogue cameras because they do not require a separate cable run or power boost to send images over a longer distance.

Wireless CCTV camera - Not all wireless cameras are IP-based. Some wireless cameras can use alternative modes of wireless transmission, but no matter what the transmission method, the primary benefit to these units is still the same, extreme flexibility in installation.

High-Definition (HD) CCTV camera - Ultra high-definition cameras are often relegated to niche markets, such as casinos and banks. These give the operators the ability to zoom in with extreme clarity (to look at a poker player who might have something up their sleeve).

Beyond this list, there are many other types of CCTV cameras, but most of those are more related to the application in which the unit will be used versus the type of camera.

When deciding on what camera to use at each point of the installation, consider the camera resolution. Camera resolution is measured in Megapixels (MP). Higher resolution generally means more image detail. A rough guide can be, considering the distance from the camera location to the point of interest - up to 10 metres - 2 MP; up to 20 metres - 3MP; up to 30 metres - 4MP.

The type of camera should be considered carefully as the end product and price differs greatly eg. is the vision needed for court purposes to identify a person clearly, or is it a means of merely alerting you to a person in the area?

POSITIONING OF CAMERAS

Cameras should be:

- In places where offenders are most likely to pass or gain access, such as building entry or exit points, cash registers, rear storerooms or areas where high value items are kept;
- Clearly visible if seeking to deter potential offenders;
- Placed at a height that captures a full view of the offender's face while not being obscured by other interferences;
- In areas where image capture will not be compromised by insufficient lighting.

For CCTV to be useful for police purposes, the largest possible facial image of an offender is required. The usefulness of facial images captured is largely dependent upon the quality and placement of cameras. Do not position cameras at heights that only provide vision of the top of a person's head.

In the event of a crime, please advise police that your premises has a CCTV system installed.

RECORDING

All camera footage is recorded onto a Video Recorder via hard drive/s which ideally has enough recording space for 30 days. Most systems nowadays have remote access to recorded footage via PC software or an app.

It is important that employees know how to operate security equipment and that it is regularly tested and checked.

WHO NEEDS TO BE ADVISED THAT CCTV HAS BEEN INSTALLED

There is no mandatory or centralised CCTV register for privately owned households or business CCTV systems in Victoria. However some police stations may have their own localised registers.

FURTHER INFORMATION

Further information to assist your business is available from the following sites:

Victoria Police Crime Prevention

police.vic.gov.au/communitysafety

Victorian Surveillance Devices Act 1999

legislation.vic.gov.au

Privacy Act 1988 (Fed)

legislation.gov.au

Community Crime Prevention

crimeprevention.vic.gov.au

Victorian Ombudsman CCTV in Public Place guide

prov.vic.gov.au/government/standards-and-policy

COUNTER **TERRORISM**

Counter Terrorism is the implementation of security practices and strategies intended to reduce the risk and consequences of a terrorist attack on an organisation. Its aim is to safe-guard people, property and information.

The majority of businesses don't require an evaluation specifically regarding counter-terrorism, however, it is highly recommended that it be considered as a part of an overall security risk review. See **'Securing your Business'** to understand the level of risk your business may be exposed to and identify what security improvements may be required to protect your premises and people.

This section provides important security information; but, is not intended to replace independent, privately contracted security advice.

Any review conducted should commence at the property boundary and work inwards and consider:

- Gates and fencing inclusive of perimeter and building protection;
- Ease of access to car parks and buildings by employees, visitors and members of the public;
- Effectiveness of monitored security alarm systems and live or recorded CCTV coverage (if any), including storage capacity;
- Mail handling procedures and identification, response to suspect packages or items, incorporating evacuation procedures and incident response management;
- Risk of theft of assets or information.

The Victorian Government is committed to working with businesses to counter acts of terrorism. Details about some of the government programs to assist Victorian businesses to manage their security risks are available on the Victoria Police website: police.vic.gov.au and relate specifically to:

- Places of mass gatherings;
- Critical infrastructure;
- Chemicals of security concern.

FURTHER COUNTER TERRORISM INFORMATION AND ASSISTANCE

The Australian Government has produced a guide to help small to medium businesses with risk management planning.

The ***Good Security, Good Business*** guide provides details of how your business can minimise risks, and manage and recover from an incident, including a terrorist attack. You can download a copy of the booklet from the Australian Government Trusted Information Sharing Network website.

tisn.gov.au

National Security Hotline

1800 123 400 – is the single point of contact for the public to report possible signs of terrorism.

nationalsecurity.gov.au/securityandyourcommunity

CREDIT CARD **FRAUD**

WHAT IS FRAUD?

Fraud is behaviour that is deceptive, dishonest, corrupt or unethical.

For a fraud to exist there needs to be an offender, a victim and an absence of control or safeguards. Fraudulent activity in the workplace often results in the loss of revenue and property, while increasing operational costs and service charges. It can also mean obligations to employees, customers, suppliers or contractors can't be met.

The knock on effect for business may:

- Damage credibility;
- Compromise confidentiality;
- Result in public criticism.

With the rapid advancements in technology, frauds are becoming more sophisticated, widespread and complex. As a result, stamping out fraudulent practices becomes a huge challenge and requires extra vigilance on the part of business and individuals.

CREDIT AND DEBIT CARD PAYMENTS

Credit and debit cards are issued by banks or financial institutions. A credit card lets your customers pay for goods and services by incurring a debt with a credit card provider. Debit cards deduct the amount of money from a sale from a customer's bank account.

The difference between a credit card and debit card is not usually important for running a business. On the front, credit and debit cards have an issue date, expiry date and credit or debit card number. On the back, they usually have a security code and signature.

Some debit and credit cards have a chip for contactless payments using technologies such as MasterCard Paypass and Visa payWave. Credit and debit cards often have a Personal Identification Number (PIN) that customers need to use to authorise payments, although this can depend on the purchase amount.

BENEFITS OF CREDIT AND DEBIT CARD PAYMENTS

- Low labour costs - after short delays, debits and credit card payments go directly into your bank account. You don't need to pay people or spend time to bank credit card payments;
- Less Risk of Theft - credit and debit card payments go directly into your bank account, so there's less risk of theft;
- Credit and debit card providers keep records, which act as proof of payment. Proof of payment can help resolve disputes;
- Convenience - many customers may prefer credit and debit cards payments in preference to carrying large sums of cash.

DISADVANTAGES OF CREDIT AND DEBIT CARD PAYMENTS

- Service Fee - processing credit and debit card payments usually requires paying service fees to banks, credit unions or online third party services;
- Transaction fees - some credit and debit card providers may charge you a fee per transaction;
- Lack of privacy - credit and debit cards create a record of each transaction. Some customers may prefer cash for private goods and services, such as medications;
- Reliance on Electrical and Telecommunication infrastructure - processing credit and debit transactions requires electricity and sometimes needs access to phone networks. Cash may be more reliable if these services are unavailable or unreliable;
- Reputational risk - mishandling credit or debit information can damage your business' reputation. Make sure you keep all customers data private and secure;
- Technical Problems - machines to process credit and debit card payments can malfunction.

PREVENTION - SECURITY TIPS

- Do not enter the card details into the EFTPOS terminal manually without prior approval from the card issuer. Thieves using stolen credit cards will often damage the magnetic strip to avoid the card being identified by EFTPOS systems as stolen;
- Check card signatures;
- Check that the card numbers on the front and back of the card match;
- Make sure holograms are clearly visible, appear three dimensional and move when the card is tilted;
- Check the card is current by checking the 'valid to' date;
- Check for ghosting or shading used to cover up changed numbers;
- Ensure the transaction successfully processes before providing the goods to the customer;
- Ask for further explanation if unsure;
- It is preferable to sight the credit card being used, but if accepting credit card payments over the telephone or internet, request the customer quote the three or four digit security number printed on the back of the card, and seek approval via the telephone from the card issuer;
- If taking telephone or internet purchases,request a landline number in preference to a mobile number;
- Ensure credit card slips are disposed of in locked waste bins or shredded prior to disposal to prevent criminals from obtaining customer credit card details;
- If you have any doubts, ask to see a form of photo identification and ensure the person presenting the card is the rightful cardholder;

- If the transaction is not authorised:
  - Hold onto the card;
  - Ask for additional photo identification;
  - Contact police on **Triple Zero (000)** if required.
- Contact the Card Authorisation Centre to obtain authorisation for credit card transactions when:
  - The value of the transaction exceeds your floor limit;
  - When conducting a manual or off line transaction.
- Set an appropriate limit for refund or cashback for each EFTPOS terminal;
- Change regularly and keep confidential the EFTPOS password or pin;
- Maintain physical security of EFTPOS terminals;
- Switch off your EFTPOS machines at night.

CUSTOMER CONSIDERATIONS

Be alert for customers who:

- Appear anxious;
- Arrive on closing time;
- Have no identification;
- Appear in a hurry;
- Purchase large quantities of goods or expensive items;
- Request transactions to be entered manually.

If you suspect the card has been altered, or have any doubts about the person presenting it:

- Keep the card;
- Check the warning bulletin to see if the number is listed;
- Ask for additional identification;
- Call your supervisor;
- Contact the Card Authorisation Centre to verify information;
- If still suspicious, contact police on **Triple Zero (000)**.

FURTHER INFORMATION

Further information to assist your business is available from the following sites:

Victoria Police Crime Prevention

police.vic.gov.au/communitysafety

Australian Institute of Criminology

aic.gov.au

Visa Card

visa.com

Master Card

mastercard.com.au

American Express

americanexpress.com

ELECTRONIC **CRIME**

E-Crime is a general term used to classify the investigation of criminal offences, where computers or other electronic devices have been utilised in some manner to facilitate the commission of an offence. The opportunity to commit E-Crimes is increasing, aided by enhanced technological capability and availability of devices such as computers, mobile telephones, MP3 players and digital cameras.

Increasingly, many small businesses and retailers are opening their business and telephone lines to customers and suppliers through electronic trading. Coupled with the many benefits that electronic trading provides, it can however expose a business to unique methods of crime involving the business, suppliers and customers.

Some of the more common offences committed via this medium include, credit card fraud, online auction fraud, computer hacking, and the forwarding of offensive, menacing or harassing e-mails. E-Crimes can range from very simple crimes to immensely complex ones. The types of crime include:

- Unauthorised access;
- Denial of service;
- Cyber stalking;
- Identity theft;
- Fraud;
- Possession of illegal material.

The motives for E-Crime can include:

- Attention seeking;
- Concealment of crime;
- Sexual;
- Intimidation;
- Malicious destruction;
- Curiosity;
- Profit or personal gain;
- Revenge or vengeance;
- Terrorism.

You can protect yourself and your business by learning how to recognise the danger signs of E-crime. Some matters may appear on the surface to be criminal offences, however this is not always true and you may only have recourse via civil action. There is national and state legislation available to assist law enforcement agencies in the prosecution of offenders for these types of offences. These agencies have the prerequisite skills and resources available to effectively coordinate and investigate these matters.

If you find you are the victim of E-Crime it is important to report the matter quickly to police - this can be accomplished online by accessing 'ACORN' (see heading ACORN).

HOW CAN I PROTECT MY BUSINESS

It is important to put in place measures to reduce risk and protect business information. If your business does not have a person skilled in IT, then it may be a worthwhile investment to have an IT qualified person or company to assist with setting up safeguards for your computer system (these are readily obtainable from online searches or local publications).

There are many products on the market that may be recommended and installed to give you a good level of security. The security of your system needs to be regularly scrutinised and updated to ensure advancements in technology don't make your security measures obsolete.

BASIC SECURITY TIPS

- Install reputable anti-virus and anti-malware software and keep it up to date;
- Install reputable firewall software and keep it up to date;
- Keep software patched and up to date;
- Passwords should be confidential, complex and regularly changed;
- Immediately remove internal / external network access of employees leaving employment for whatever reason;
- Where you suspect that your network / access password has become known to a third party, change it immediately;
- Do not leave your computer logged in to the network whilst you are not present (log off or lock your computer);
- Where possible consider setting a short time out on your screen saver and ensure that log in is required to recover from the screen saver;
- Delete any suspicious e-mails without opening - curiosity is a tool often used to hack a computer system or send a virus;
- Do not open e-mail attachments which have not been scanned for virus / malware, or have been received from an unknown source;
- Only download software from reputable sources;
- Backup critical data and keep it separate from your Internet connected computers. Regularly copy the data to a back up device;
- Test that you can recover the information using that back up device.

HOW DO I KNOW IF MY BUSINESS HAS BEEN COMPROMISED

The following is a useful list of potential indicators which may indicate the presence of hackers within your computer system:

- Your computer system performance is unusually and exceptionally slow for no apparent reason;
- There is odd activity in a computer log, activity at unexpected times or to unexplained sites. There is an unexplained large increase in web traffic to / from your web site. The more it is investigated, the more you suspect that something is wrong;
- Your anti malware / anti-virus software, task manager or registry, editor is disabled and can't be started or does not appear to be functioning, or you receive fake anti-virus messages;

- Your bank accounts are missing money, or you get calls from stores about non-payment of shipped goods, or established business procedures do not appear to have been followed and transactions are unexplainable;
- Fake e-mails have been sent from your account or you are no longer receiving e-mails and no one is receiving e-mails you have sent;
- There are new software installs on your computer that you didn't install. Your password has been changed and / or you can't access your network. Unwanted browser toolbars unexplainably appear. Internet searches are redirected to other sites. Frequent random pop ups suddenly start appearing on your site.

ONLINE FRAUD

If you believe that you have been the victim of an online auction fraud, immediately report the matter to the auction company (i.e. eBay, Gumtree etc.). Most online auction houses have an identified process for reporting and following up suspect transactions, and can often assist you to recover your property and provide you with the records that you will need to report the matter to police if a crime is identified.

If you become the victim of online fraud, the matter can be reported to police via an online portal, 'ACORN'. Ensure that you preserve any electronic evidence (logs, e-mails or other communications between yourself and the suspect) relating to the matter. If you are confident in the process, create an electronic copy of each e-mail including all header information, and copy it to an external device. Do not delete the original e-mails; they contain valuable forensic information that is usually hidden from sight. When reporting the fraud, ensure that you provide a copy of the data to the police. In more complex matters the police will want to examine your computer.

REPORTING ELECTRONIC CRIME VIA ACORN

What is ACORN?

Cybercrime is an issue which affects many Australians. As Australia's reliance on technology grows, the cost and incidence of cybercrime is expected to increase.

The Australian Cybercrime Online Reporting Network (ACORN) is a national policing initiative of Commonwealth, State and Territory governments. It is a national online system that allows the public to securely report instances of cybercrime and provides advice to help people recognise and avoid common types of cybercrime.

ACORN is a key initiative under the national plan to combat Cybercrime, which sets out how Australian agencies are working together to make Australia a harder target for cybercriminals. ACORN has been designed to make it easier to report cybercrime and help develop a better understanding of the types of cybercrime affecting Australians.

By understanding the enablers of cybercrime, we can make it harder and less rewarding to commit cybercrime.

ACORN is a secure reporting and referral service for cybercrime and online incidents which may be in breach of Australian law. Certain reports will be directed to Australian law enforcement and government agencies for further investigation.

What Can I Report on ACORN

Common types of cybercrime include hacking, scams, fraud, identity theft, attacks on computer systems and illegal or prohibited online content.

If you are concerned about your immediate safety you should contact **Triple Zero (000)** before continuing with an ACORN report.

How Do I Make a Report

ACORN can be accessed at acorn.gov.au

The screens will then guide you to make a report. Provide as much detail as possible so ACORN can best process your report. You should keep any relevant information about the incident in case police contact you. This could include e-mails, screenshots or any other evidence in your possession.

You should not provide any personal financial details when reporting. You should not make a report on a device which you think might be infected by a virus.

The report must be completed in one session and will automatically close after 5 hours of inactivity.

What Happens Next

Shortly after you submit your report, you will receive a confirmation e-mail with a unique ACORN reference number if you provide your e-mail address.

Please be aware that not all reports to ACORN will be referred or investigated. However, your report will be treated seriously and will help our law enforcement and government agencies to develop a clearer picture of cybercrime trends affecting Australians.

While ACORN accepts anonymous reports, the site logs IP addresses of all reports received. This is to ensure that malicious reporting can be detected and acted on.

FURTHER INFORMATION

Further information to assist your business is available from the following sites:

Victoria Police Crime Prevention
police.vic.gov.au/communitysafety

Australian Institute of Criminology
aic.gov.au

ACORN
acorn.gov.au

Australian Federal Police Online Fraud and Scams
afp.gov.au/what-we-do/crime-types/cybercrime/online-fraud-and-scams

Scam Watch scamwatch.gov.au

SECURING YOUR **BUSINESS**

There are many forms of crime that affect businesses. Identifying security issues and taking some simple crime prevention steps can reduce the risk of crime for business, employees and customers. This section provides important security information and advice, however, it is not intended to replace independent, privately contracted security advice.

The main aim of business security is to:

- Reduce the likelihood of a business being targeted by offenders;
- Reduce the impact that crime can have on a business;
- Reduce the reward and increase the effort it would take to access the premises and goods;
- Increase the likelihood of offenders being identified and caught.

The following are some basic security tips for you to consider:

- Clearly display your business name and address at the front of your premises to help emergency services locate your property quickly;
- Ensure clear visibility inside and outside your business by using good lighting, particularly over entry / exit points;
- Keep trees and shrubs trimmed to increase visibility and reduce concealment opportunities;
- All boundary fences and gates should be well built, maintained and adequately secured. If padlocks are needed, ensure they are of an appropriate and recommended standard;
- Clear all building perimeters of rubbish and potential climbing aids;
- Fully secure all external doors and windows with good quality locking devices and ensure they are regularly maintained;
- All doors should be of solid construction and door frames fitted with steel door jamb strengtheners;
- Glass within doors and windows should be reinforced with either a shatter resistant film or laminated glass;
- Installing bollards, heavy planters or large rocks to act as a barrier to ram raids; and security bars, screens, grills or roller shutters to vulnerable windows and skylights (subject to Metropolitan Fire Brigade (MFB) approvals);
- Installation of a monitored security alarm system and surveillance cameras to deter offenders and assist police to identify offenders;
- Prominently display signs indicating the presence of a security system and other measures such as 'No cash/drugs kept on premises'; 'CCTV constantly monitoring premises';
- Install electronic sensors to advise employees when customers are entering and leaving your store;
- Ideally, stand-alone shelving should be no more than 1.6 metres high to enable visibility of customers throughout the store;
- All property of value should be secured with details of description / make / model / serial number recorded and clearly / permanently marked with your store name or Australian Business Number (ABN);
- If your business deals in cash, limit the amount of money you hold in the cash drawer and don't count money in public view;
- Never leave large amounts of cash on premises overnight. Banking should be conducted during working hours and at irregular, unpredictable times. Where this is not practicable, ensure cash is placed in a secure safe and not taken home;
- All ATMS should be placed away from entry points of your premises, be anchored to the ground and covered by CCTV surveillance cameras;
- Ensure safes are anchored to a solid object to restrict removal;
- Ensure all employees understand and adhere to lock-up procedures;
- Local police and any security provider should be advised of emergency after hour's contacts;
- Provide employees with regular training in the use of your business security measures and procedures and;
- Regularly update and review your Business Security Plan as appropriate (weekly, monthly or yearly).

KEY / ACCESS CARD CONTROL

- Must be maintained at all times to ensure internal security;
- Utilise security keys / access cards that cannot be copied without authorisation;
- Maintain a formal key / access card register, ensuring their issue and return is monitored;
- When not in use, keys / access cards should be kept in a lockable steel cabinet located in a secure area;
- Keys / access cards should be restricted to a minimum number of people and retrieved from leaving / ex-employees.

ADDITIONAL INFORMATION

Visit the Victoria Police website police.vic.gov.au/communitysafety for a 'Do It Yourself' Business Security Assessment form.

VICTORIA POLICE

Business Security Self Assessment

WELCOME TO THE VICTORIA POLICE BUSINESS SECURITY ASSESSMENT

TELEPHONE **THREATS**

TELEPHONE THREATS - BOMB AND OTHER

Although rare, telephone and bomb threats are an issue all employees should be made aware of. It is advised that a photocopied or laminated version of the 'Phone Threat Checklist' (**Appendix B**) be left directly beside or near business telephones for immediate use by employees should a threatening phone call be received.

THE PROCEDURES DETAILED BELOW SHOULD BE CLEARLY EXPLAINED AND FOLLOWED BY ALL EMPLOYEES

Employees should be instructed that if they receive a threat, they should:

- Stay calm;
- Do not panic or make return threats;
- If possible, fill out all information on the 'Phone Threat Checklist' while on the phone to the caller;
- Listen carefully to obtain a full description of:
  - Sex of the caller;
  - Age of the caller;
  - Any accents or speech impediments;
  - Any background noises;
  - Any key phrases used by the caller.
- Ask the caller:
  - What is the threat?
  - When will the threat be carried out?
  - Where is the threat located?
  - Why is the threat being made?
- Keep the caller talking for as long as possible (to obtain as much information as possible);
- While not alerting the caller, have a co-worker inform management and immediately contact police on **Triple Zero (000)** using a separate telephone line or mobile phone;
- Once a call is finished **DO NOT HANG UP** – it may be possible to trace the call if the telephone line is kept open, regardless of whether the caller hangs up;
- Ensure all information has been written down.

LOCATING AN ITEM

If an item or suspect package is located:

- Do not touch, tilt or tamper with the item;
- Contact police immediately on **Triple Zero (000)** and follow the instructions they give.

EVACUATION

If evacuation is deemed necessary by management or police, it should be conducted in a pre-planned manner:

- Clear the immediate area within the vicinity of the item or package of all people, ensuring they are not directed past the item or package;
- Ensure people who have been evacuated are moved to a safe, designated place;
- Complete an evacuation record sheet to ensure all employees are accounted for;
- Ask the call taker to remain available at the designated location to assist police.

THEFT BY **EMPLOYEES**

An unfortunate aspect of owning and managing any business is the issue of theft by employees. Theft by employees can be committed in a number of ways and while it cannot be totally prevented, implementing some simple prevention strategies can go some way toward reducing this problem.

PREVENTION

- All applications for employment should be carefully screened including the sighting of original photographic identification and a check of references (any unexplained gaps in past employment should be investigated);
- Consider ongoing and regular National Police Criminal History checks, particularly for new employees;
- An induction program for new employees should be conducted providing a clear understanding of security procedures, policies, acceptable and non-acceptable behaviour, and consequences for breaches;
- Openly communicate and promote to employees the preferred process for purchasing goods from your business by employees, family and friends;
- Have an effective asset inventory control system to identify and immediately act regarding losses as they occur such as short falls in daily takings;
- Demonstrate and provide strong and consistent supervision of all employees and immediately deal with issues of concern;
- Managers need to be scrutinised carefully as they generally have more extensive access to cash handling;
- Utilise appropriate security provisions that make theft more difficult and increase the likelihood of employees getting caught (such as CCTV). Ensure employees are aware they are under continuous observation;
- Adopt a prosecution policy when dealing with employees. A widely publicised successful prosecution in court can act as an effective deterrent for others;
- Provide a designated area where employees can safely lock away their personal belongings;
- Maintain strict key or access card control to ensure internal security;
- Careful checks should be made at dispatch and delivery areas to reduce the possibility of falsification of records, theft and signs of collusion between drivers and employees;
- Watch for customers who continually return to the same register or employee, or appear to be over friendly or familiar with employees;
- Consider undertaking spot checks of bags if required;
- Recognise and reward employees loyalty and ongoing honourable behaviour;
- Provide ongoing retail security training programs to all employees;
- Encourage employee contributions to retail security initiatives.

REMEMBER: Most employees are loyal to their employers and will work very hard and diligently on their behalf, especially if appropriate reward and recognition exists within the business.

THEFT FROM **SHOP**

Theft accounts for a large percentage of reported annual shop losses. Shop stealing is sometimes referred to as shoplifting but no matter what you call it, if somebody takes something from your store that they have not paid for, it is theft.

Shoplifters come from all walks of life and socio-economic backgrounds. They generally fall into one of two groups: amateurs or professionals.

- Amateur shoplifters usually steal on impulse (i.e. young people who steal to impress their friends).
- Professional shoplifters are more likely to work in pairs or groups but may work alone. They often case out a store before stealing and usually 'steal to order', or to obtain a false refund for the items they have stolen.

PREVENTION

- Acknowledge all customers – customer service is one of the most effective crime prevention strategies;
- Pay attention to customers who are nervous or appear distracted around merchandise;
- If store security or loss prevention officers are employed, familiarise employees with their identity, when they operate and how they are to be contacted;
- Approach people who stand around restricted areas, restrooms, stockrooms or stairways;
- Be aware of people wearing loose overcoats and bulky clothing, especially in hot weather;
- Approach and query persons claiming to be tradespersons, particularly in unauthorised areas. Consider requesting to inspect trade related identification;
- Be mindful that prams, shopping trolleys, boxes and bags can be used by shoplifters to conceal goods they are attempting to steal;
- Check the number of items taken in and out of changing rooms;
- Ensure empty hangers and excess stock is removed from racks and shelves;
- Ensure employees are familiar with the items / quantities of stock on display;
- Keep customers in view at all times and be conscious of having your back to customers;
- Never leave the sales area or cash registers unattended.

STORE LAYOUT AND DESIGN

- Limit the number of entry and exit points to your store;
- Your store layout should be well-lit and as open as possible providing good visibility to all areas;
- If possible, elevate the cash register and counter area to improve employee view of the shop;
- Employees should have a clear line of sight along rows of shelving or display racks. If blind spots occur, install convex mirrors or mirror tiles behind stock shelving or consider installing CCTV;
- Ensure customers have no direct access behind the counter;
- Ideally, place cash registers close to store entry or exit points to prevent easy removal of money by offenders;
- Ensure all selling areas are adequately lit;
- Where possible, lock expensive and easily portable goods in cabinets close to employees working areas;
- Stock and shelves should be neatly stacked with price tickets properly secured to goods to prevent removal or switching for cheaper priced items;
- Clearly display warning signs regarding security measures in place at your store, your bag checking policy and the consequences of theft;
- Ensure there are clearly defined public and private areas of your store and keep employees rooms and stock rooms locked at all times;

DETECTION

Things to look out for:

- Hands – they do the stealing;
- Customers who don't appear to have a deliberate purpose to purchase items;
- Customers who remain in the store for lengthy periods of time, or who are 'sampling' merchandise that does not fit with their character;
- Customers who appear nervous, perspiring heavily, are agitated or won't make eye contact with you;
- Organised distractions where there are one or more (or a group of) persons attempting to commit thefts whilst distracting employees;
- Unsupervised children who are in the store during school holidays.

APPREHENSION

Retail employees have a lawful right to apprehend persons they see or witness committing a theft in their store. An arrest can only be affected on a person found committing an offence and the apprehension of a thief should always be made by the employee who has witnessed the theft, and preferably in company with another employee.

- It is important that a set of procedures are put in place and employees adhere to these procedures to prevent possible legal ramifications in the event of an unlawful arrest.
- The only occasion this does not apply, is if another employee has observed the theft, say on CCTV, and has then relayed this information to another employee.

IF YOU WITNESS AN OFFENCE:

The employee who witnessed the offence **must** be sure of:

- Seeing the goods being taken;
- Seeing where the person placed or concealed the item/s;
- Not losing sight of the suspect at any time;
- The stolen item or items are still in the possession of the suspect and have not been thrown away, dropped, dumped or paid for;
- The suspect has passed the last point of payment and made no attempt to pay for the item or items;
- While it may be lawful to arrest a person in certain situations, it is recommended and good practice to have that person assist voluntarily;
- Contact police on **Triple Zero (000)** and await their attendance.

Co-operation is a better strategy than the possible legal ramifications associated with an arrest - it is recommended that independent legal advice be sought about making arrests in this regard.

If the suspected shoplifter agrees to remain with you:

- Explain who you are (eg. the manager, store security guard) and show identification;
- Tell the person why they are being spoken to and ask them to accompany you back into the store.

A good approach to stopping a suspect is to say something similar to:

"I believe you have some merchandise on your person or in your bag, which you may not have paid for. We would appreciate you coming back to the store to straighten out this matter."

- You do not have a legal right to use force unless the person has been arrested (force in this sense means a degree of force any reasonable person would use if faced with the same situation);
- It is recommended that you do not physically touch the suspected shoplifter;
- Advise the person that the police will be called;
- Ask the person to surrender any property that does not rightfully belong to them;
- You are not entitled to conduct searches of the person;
- Contact police on **Triple Zero (000)** and await their arrival.

If the situation causes danger to you, your employees or customers do not approach the shoplifter – the value of goods you are attempting to recover can never exceed the value of your life.

IF IN DOUBT - DO NOT APPREHEND

A WRONGFUL ARREST MAY LEAD TO CRIMINAL OR CIVIL LITIGATION BY THE CUSTOMER

VANDALISM

Vandalism is the wilful destruction or damage of property, which defaces or otherwise adds a physical blemish that diminishes the property's value.

Vandalism includes:

- Breaking a building's windows;
- Carving initials into public park trees or public benches;
- Keying a car or puncturing its tyres;
- Graffiti – the use of spray cans, permanent marker pens or sharp objects to mark or etch walls, fences or windows with a 'tag' usually depicting the initials or nickname of the person responsible or an offensive slogan.

STRATEGIES TO MINIMISE OPPORTUNITIES FOR VANDALISM AND GRAFFITI AT YOUR BUSINESS PREMISES:

- Ensure your premises is well lit and fitted with movement activated lighting in areas most at risk. Consider installing security cages on external lights and speakers;
- Prominently display warning signs indicating the presence of a security monitoring system (CCTV) and in relation to trespass and potential prosecution;
- Replace window glazing with a damage resistant material such as polycarbonates;
- Remove rocks, debris, flammable material and any object that can be used to cause damage;
- Install fences or plant vegetation to make graffiti prone areas difficult to access;
- 'Remove the canvas' – cover graffiti prone areas with named gardens, murals or mosaics as most legitimate street artists follow basic rules to only use free walls and respect other artists – 'If the art is really good, you don't touch it';
- Develop a close relationship with your local traders' association, local police and council and make positive use of casual (natural) surveillance by involving neighbours, other local traders and community crime prevention groups;
- No matter how small or insignificant the graffiti is it should be removed as quickly as possible as continual, immediate removal has proven to be the only successful measure to deter graffiti artists by reducing exposure time;
- Your local council may have a graffiti hotline to assist with cleaning and removal. Contact your local council for more information.

For a guide to the differences between graffiti and street art, the City of Melbourne has a comprehensive website with an image library.

Visit the City of Melbourne website at melbourne.vic.gov.au for **'Graffiti and Street Art'** information.

Vandalism can be intentional or may result from people using the environment and adapting it to make it function better for them.

Some examples include:

- Short cuts across lawns;
- Broken windows near ball playing areas;
- Holes in fences to create short cuts.

The offender may have had no intention of causing the damage, nor do they perceive it as damage, but others see the results as vandalism.

ADDITIONAL INFORMATION

To further assist you in reducing vandalism, complete a 'Do It Yourself' Business Security Assessment available from the Victoria Police website police.vic.gov.au/communitysafety.