



Ver. 2.6 - September 2017

PERSONAL SECURITY HANDBOOK

2nd Edition

*Protecting
what matters
most!*

(Page intentionally left blank)

Table of Contents

▪ Introduction	5
○ Security 101 (the basics)	6
○ Risks / Risk Perceptions	6
▪ Workplace Security	7
○ General Safety	7
○ Suspicious Packages or Mail	8
○ Using elevators, escalators and stairs	9
○ Workplace violence	10
○ Dealing with complex clients	18
○ Inappropriate Conduct & Communications	19
○ Active Assailant / Shooter	22
▪ Telephone Security	26
▪ Home Security	27
○ Be Suspicious	27
○ While Away	28
○ Answering Your Door	28
○ Exterior Grounds	28
○ Entrances and Exits	29
○ Interior Features	29
○ Other Desirable Features	29
○ Mail and Newspaper Security	29
○ Special Precaution for Children	30
▪ Internet / Social Media / Identity Theft	31
○ Identify Theft	31
○ Introduction of Malware	31
○ Social Engineering Attacks	32
○ Avoiding Fraudulent Usage of Social Media	32
○ Social Media and Children	34
▪ Personal Security Precautions	35
○ General	35
○ Running / Walking / Working Out	35
○ Using Bank Machines	36
○ Social / Business outings	36

Vehicle Security	37
○ General.....	37
○ Maintenance	37
○ Before Entering.....	37
○ While Driving	38
○ Parking	38
○ Stranded.....	38
○ Being Followed	39
○ Road Rage	39
➤ How to Avoid	39
➤ If you are a victim	39
 ▪ Public Transportation Security	 40
○ Bus	40
○ Taxi.....	41
○ Plane	41
 ▪ Acknowledgements	 42

Introduction



“OUR

SECURITY MUST BE THREATENED IN ORDER FOR US TO APPRECIATE IT” - Mary Astor

Welcome to our 2nd edition of the Personal Security Handbook. Thanks to you, our valued stakeholders, we received some tremendous feedback since our initial release in July of 2016. This reflects one of our most cherished philosophies; security is everyone’s responsibility. In that light please note, this is your handbook, and we will always remain receptive to your thoughts, your comments and your experiences. So please keep sharing and improving this product.

This Personal Security Handbook is intended for all Government of Alberta employees. The handbook was produced in good faith based on best practices from a multitude of different sources. It offers a variety of suggestions that will better inform you about your personal security while at work, traveling to and from work and at home.



Peter Lemieux
Director, Corporate Security Services
Corporate.Security@gov.ab.ca



Corporate Security Services

Security 101 (the basics)

In order to truly benefit from the insights contained in this booklet, it is necessary to have a basic understanding of security, its key concepts and philosophies.

Safety & Security

Quite often you will hear Safety and Security used interchangeably, but did you know there is a difference between the two terms?

- **Safety** is about fostering an environment that is relatively free from hazards that has the potential to cause injury. Hazards at the workplace can include noisy equipment or machinery, electricity, chemicals or workplace violence.
- **Security** is about applying protective measures to reduce Human Induced Intentional risks. In other words preventing an individual or group from causing harms such as violence, theft or willful damage.

Risk

The level of Risk is measured based on the likelihood and impact of an adverse event. In security jargon: (Risk = Likelihood + Impact).

So let's look at a worst case scenario...an active assailant / shooter in a government facility. Although the impact to employees would be significant, the likelihood of it occurring is very rare. So the risk of this type of event is determined to be low. In some instances, the 'risks' can be slightly elevated so we will have to implement other measures to offset these increased risks such as reinforced barriers or perimeter screening.

Perception of Risk

Perhaps the greatest challenge to security is how we individually perceive risks. Our perceptions are formulated and influenced by a number of different factors. Human induced intentional events for example, are overstated over natural events or disasters. This can often be attributed to how the media portrays events.

The potential for violence to you or your family is an important subject. While it rarely occurs, we still need to remain vigilant and be better informed to take sensible precautions.

Workplace Security

General

- Familiarize yourself with your workplace security and facility emergency response policy / plan.
- Central reception at work should handle visitors and packages.
- Avoid isolated or deserted stairways.
- Lock up your valuables.
- Follow a clean desk policy.
- Do not prop open entrance or secure doors.
- Report suspicious tampering with physical security (doors, windows, locks, etc.).
- Ensure your building access pass remains visible when in controlled areas.
- Be aware of unfamiliar persons in your area and report suspicious persons to your immediate supervisor.
- Report all thefts and security incidents.
- Keep items off the front counter that could be used as weapons.
- If working after hours, keep all doors and windows locked and try to coordinate with other co-workers who might be working late as well.
- When you finish work, go to your vehicles together. Ensure the others are safely in their vehicle and on their way before you leave. Leave the parking lot together.
- If the building or company has on-site security, advise them you're working late and ask if they can check in on you periodically.
- Consider advising security when you're leaving.
- Consider asking if they are available to escort you to your vehicle.
- If alone, contact your family/friend and advise them you'll be working late and will call before you leave and advise them of your route home.
- Have your name removed from reserved parking area.
- Watch for "tailgating" on foot or by vehicle (secure access parking garage).
- Pay attention to:
 - Persons in building loitering;
 - Persons who appear to have no need for, but are requesting sensitive information, such as information on security;
 - Persons wearing clothing not consistent with weather conditions (bulky jacket in 90-degree weather);
 - Persons monitoring areas, taking pictures of buildings and entrances, making diagrams;
 - Persons attempting to access utility locations; or
 - Something about the person(s) just doesn't seem right.
- When an unfamiliar / unauthorized person comes into your office it is important to challenge that person. There are four words which will enhance the security of your office... **"May I Help You?"**
- An unknown person should not be allowed to move through office space without an escort.

- Know who has access to your office. "If you see something - say something"
- At the office or out of the office, at work or on your own leisure you must train yourself to perceive through your senses (hearing, sight, smell) to be fully aware of your surroundings.
- Know your environment. Check with co-workers, security, law enforcement (crime mapping web sites) about incidents in the area, building parking lot / parkade etc. Try to stay informed on what's been happening and inform others.

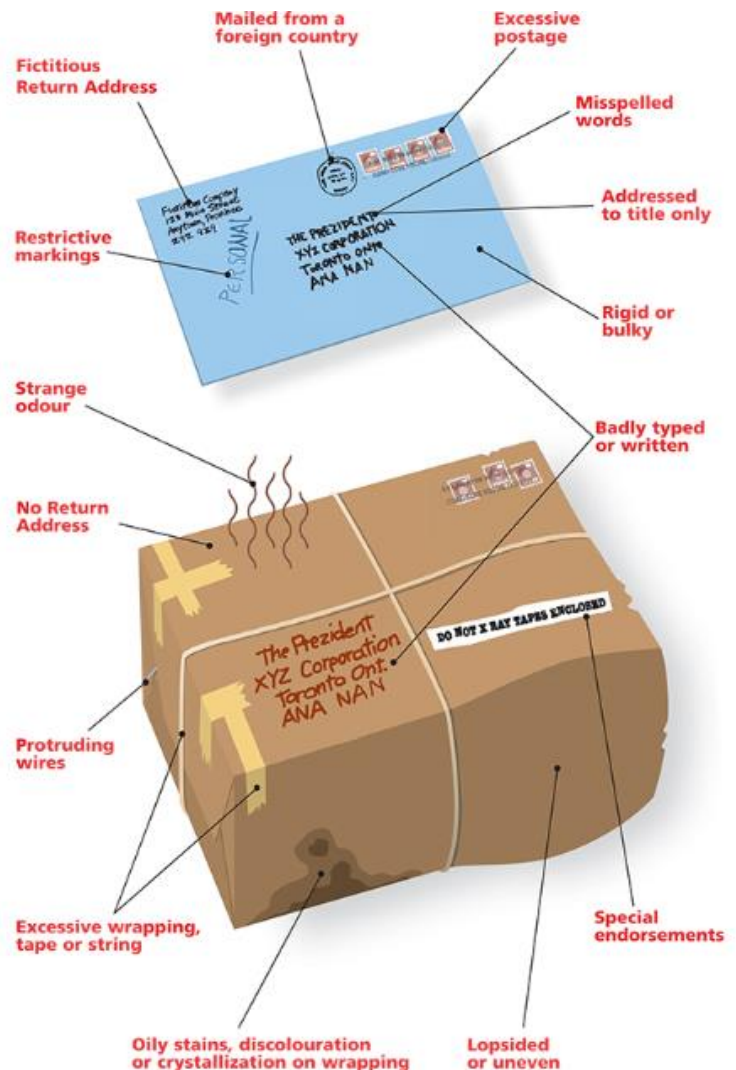
Suspicious packages or mail

Suspicious characteristics to look for include:

- An unusual or unknown place of origin;
- No return address;
- An excessive amount of postage;
- Oily stain or grease marks on the package;
- Wires or strings protruding from or attached to an item;
- Incorrect spelling on a package label;
- Differing return address and postmark;
- Appearance of foreign-style handwriting;
- Has a peculiar odor;
- Unusual heaviness or lightness;
- Uneven balance or shape; or
- Springiness in the top, bottom, or sides.

If package is suspect:

- Contact your supervisor.
- Contact Security (if they are on site) or call the law enforcement for further direction advising them of your suspicions and follow their direction.



Using Elevator / Escalators / Stairs

- While waiting for an elevator, stand off to the side; this gives you the opportunity to view inside and removes your obligation to enter if you are unsure of the occupants.
- If in doubt about person or persons inside an elevator do not get on; wait for the next one.
- If someone gets on the elevator after you and you're not comfortable with them, get off.
- Consider standing in a position to the side by the control panel, slightly angled to view others in the elevator.
- If confronted, push all the floor buttons and the emergency button.
- Unless there is an emergency, avoid pressing the stop button; you may get trapped between floors.
- When using an escalator only carry packages in one hand.
- Stand with your feet on two separate escalator steps to increase your stability.
- Give yourself appropriate space between you and the person in front of you when getting on the escalator.
- Always look who is behind you and if they are too close move up or down up to increase space/distance.
- When using stairs only carry packages in one hand.
- Walk to the outside of the stairway to increase your field of view up the stairs or around the landing.
- Avoid stopping or having a conversation on stairs.



Workplace Violence

According to the *Occupational Health and Safety Code*, Part 1, workplace violence means: "the threatened, attempted or actual conduct of a person that causes or is likely to cause physical injury".

Employees must notify their supervisor of all incidents of workplace violence even if there was no physical injury as per the Government of Alberta Occupational Health and Safety Program. Examples of workplace violence include the following:

- Threatening behaviour such as shaking fists, destroying property or throwing objects
- Verbal or written threats (any expression of intent to cause harm)
- Physical attacks such as hitting, shoving, pushing or kicking

Most people think of workplace violence as a physical assault. However, workplace violence is a much broader problem. It includes any act in which a person is abused, threatened, intimidated or assaulted in their employment. Examples include:

- Threatening behaviour – such as shaking fists, destroying property or throwing objects.
- Verbal or written threats – any expression of an intent to inflict harm, including:
 - Direct threats – clear and explicit communication which distinctly indicates that the potential offender intends to do harm, e.g. "I am going to make you pay for what you did to me."
 - Indirect threat – threats made through a third party
 - Conditional threats – e.g. "If you don't help me, you will regret it."
 - Veiled threats – usually involve body language or behaviours that leave little doubt in the mind of the victim that the perpetrator intends harm, e.g. "Do you think anyone would care if someone beat up the boss?"
- Harassment – any behaviour that is designed to trouble or worry the victim (including sexual, religious and racial), or coercive or fear inducing behaviour.
- Verbal abuse – including swearing, insults or condescending language.
- Physical attacks – including hitting, shoving, pushing or kicking the victim.

Workplace violence can be triggered by people you come in contact with in your daily work life, i.e. fellow employees, supervisors, customers, clients etc... Workplace violence is not limited to incidents which occur within a workplace. Work-related violence can also occur at off-site business related functions, such as conferences, trade shows, or social events related to work, public places; or in client's' homes. It can also include violence that occurs away from work, but resulting from work.



What Factors Increase the Risk of Workplace Violence?

- Certain work processes, situations and interactions can put people at risk from workplace violence:
 - Working directly with the public
 - Providing service, care, advice or education
 - Working alone in a remote area or in small numbers.
 - Having a mobile workplace (e.g. company vehicle , trailer)
- Risk of violence may be greater at certain times of the day, night or year:
 - The late hours of the night or early hours of the morning.
 - Specific times of the day, day of the week or month.
 - In times of certain business or organizational activities that may increase stress, such as objective performance reviews, contract negotiations, labour disputes.
- Risk of violence may be greater because of the geographic location of the workplace.

The one thing gleaned through research on workplace violence is there are warning signs that could indicate when a person or situation has the potential to become violent.

Warning Signs

Physical signs of a potentially violent person - Use caution if someone exhibits one or more of the following non-verbal signs or body language:

- Red-faced, exaggerated or violent gestures.
- Sweating, pacing.
- Restless or repetitive movements trembling or shaking.
- Clenched jaws or fists, facial grimacing.
- Change in voice, loud talking or chanting.
- Shallow, rapid breathing, scowling, use of abusive language.
- Glaring or avoiding eye contact.
- Violating your personal space.



NOTE: * Some of these signs may also be related to certain health issues

- A random act of violence or crime-related violence is often sudden and unpredictable. There may be few or no warning signs. However, in some cases there has been a clear pattern of warning signs. No one can predict human behaviour, and there is no specific profile of a potentially violent person. Nevertheless, a potentially violent person may exhibit any or all of the following characteristics:
 - History of violence.
 - Fascination with weapons, acts of violence, or both.
 - Demonstrates violence towards inanimate objects.
 - Evidence of prior violent behaviour.
 - Threatening behaviour.
 - States intention to hurt someone (verbal or written threat).
 - Holds grudges.
 - Excessive behaviour (phone calls, gift-giving).
 - Escalating threats that appear well-planned.
 - A preoccupation with violence.
 - Intimidating behaviour.
 - Argumentative.
 - Displays unwarranted anger.
 - Easily frustrated.
 - Uncooperative, impulsive.
 - Challenges peers and authority figures.
 - Increase in personal stress.
 - An unreciprocated, romantic obsession.
 - Serious family or financial problems.
 - Recently lost their job.
 - Negative personality characteristics.
 - Suspicious of others.
 - Believes he or she is entitled to something.
 - Cannot take criticism.
 - Feels victimized.
 - Shows a lack of concern for the safety and well-being of others.
 - Has low self-esteem.
 - Blames others for their problems or mistakes.
 - Marked changes in mood or behaviour.
 - Extreme or bizarre behaviour.
 - Irrational beliefs and ideas.
 - Appears depressed.

- Expresses hopelessness or heightened anxiety.
- Demonstrates a drastic change in belief systems.
- Marked decline in work performance.
- Socially isolated.
 - History of negative interpersonal relationships.
 - Few friends or family.
 - Sees the company as a “family.”
 - Has an obsessive involvement with their job.
- Abuses drugs or alcohol.

If you are concerned about an individual, who exhibits some of the above characteristics, - **TAKE ACTION**. Obtain assistance from any of the following: your supervisor, your manager, Human Resources, Corporate Security Services, and/or the Employee Assistance Program. For more information on employee assistance, see <https://www.shepell.com/en-ca/totalhealthsolutions/yourefap/>

Common Characteristics of Violent Incidents between Employees

Violence usually begins as a verbal dispute and almost always involves people who know each other. Disputes often appear to have relatively trivial causes. The dispute pattern is usually not random and unique; rather, it builds, intensifies and continues. Eventual victims may behave in an irritating manner prior to a violent incident. Frequently they misjudge their own ability to arouse hostility in others, and are unaware that they are provoking a serious response to their behaviour. One should stop verbal disputes before the situation escalates.

Take all threats seriously. Depending on your situation, some or all of the following measures may be appropriate.

- If a threat has been received by a co-worker, immediately inform your supervisor / manager.
- Assist with safe transportation by:
 - Having someone escort the employee to their vehicle.
 - Arranging for someone to drive the employee to and from work.
- Ensure the employee informs their children’s school and neighbours of any threats involving the children.
- Make all staff in the office or area aware of the threats so that team supports can be put in place. Provide a description of the person who issued the threat.
- If the threat was made by a client:
 - Think about transferring the client’s file to another location and have someone formally advise the client that they are not to return to the office or contact the threatened employee again.

- Re-assign the employee to another case or assignment to avoid further contact with the threatening client.
- Support the employee if they are laying police charges and/or applying for a restraining order.
- Provide Employee Assistance Program debriefing and/or counselling to the employee and their family, if necessary.

As public service employees, we deal with Albertans on a daily basis. Most of these interactions occur without incident; however, in a few, rare cases, a client may exhibit aggressive behaviour and many employees simply do not know what to do. The next few points are some basic tips when dealing with a potentially violent person:

- *Tips for Verbal Communication*
 - Focus your attention on the other person to let them know you are interested in what they have to say.
 - Remain calm and try to calm the other person.
 - Avoid allowing the other person's anger to become your anger.
 - Remain conscious of how you are delivering your words.
 - Speak slowly, quietly and confidently.
 - Speak simply. Avoid relying on official language or complex terminology.
 - Avoid communicating a lot of technical or complicated information when emotions are high.
 - Listen carefully. Avoid interrupting or offer unsolicited advice or criticism.
 - Encourage the person to talk. Avoid telling the person to relax or calm down.
 - Try to understand. Ask questions like "Help me understand why you are upset."
 - Once you think you understand, repeat it back to the person so they know you understand.
 - Remain open-minded and objective.
 - Use silence as a calming tool.
 - Use delaying tactics to give the person time to calm down, e.g. offer a drink of water
 - Identify troublemakers and learn their names.
 - Acknowledge the person's feelings. Indicate that you can see they are upset.
 - DO NOT confront, challenge, antagonize threaten, criticize or belittle.

- Tips for Non-Verbal Behaviour and Communication

- Use calm body language - relaxed posture with hands unclenched, attentive expression.
- Arrange yourself so that your exit is not blocked.
- Position yourself at a right angle rather than directly in front of the other person.
- Give the person enough physical space. This varies by culture, but normally 2-4 feet is considered an adequate distance.
- Get on the other person's physical level. If they are seated try bending over, rather than standing over them.
- DO NOT pose in a challenging stance, such as:
 - Standing directly opposite someone.
 - Putting your hands on your hips.
 - Pointing your finger.
 - Waving your arms.
 - Crossing your arms.
- DO NOT glare or stare, which may be perceived as a challenge.
- DO NOT make sudden movements which can be seen as threatening.
- If the situation does not seem to be deescalating, get assistance from security or police.



- Terminating a Negative Interaction

- Interrupt the conversation firmly but politely.
- Tell the person that you:
 - Do not like the tone of the conversation
 - Will not accept abusive treatment
 - Will end the conversation if necessary
- Tell the person that you will ask them to leave the building, or that you will leave (if working off-site).
- If the behaviour persists, end the conversation.
- Ask the person to leave the building, or leave yourself.
- If the person does not agree to leave, remove yourself from the scene and inform your manager or supervisor immediately of the incident.
- DO NOT return to the meeting if you believe the person poses a physical threat, advise other staff and have them leave the immediate area.
- Call the police. Inform your supervisor or manager.

- *Responding to an Abusive Telephone Call*

- Interrupt the conversation firmly, but politely.
- Advise the caller that you will end the call if the caller does not stop using abusive language.
- If the abuse persists, end the call (take note of the number, if possible).
- Report the incident to your supervisor or manager and if need be inform Corporate Security (be aware of the Complex Client Policy developed by Corporate Security as a management tool for abusive and disruptive clients).
- If the caller calls back, interrupt the conversation firmly, but politely. Advise the caller that you will transfer the call to your manager or supervisor, if necessary.
- The manager or supervisor should take appropriate action to resolve any misunderstanding and reinforce with the caller that abusive language or behaviour toward employees will not be tolerated.
- If needed, record the call or use a speaker phone, so that others can hear and help identify the caller.
- Inform your supervisor, your manager and if need be, inform Corporate Security and the police.

- *Responding to a Physical Attack*

If you are attacked:

- Make a scene, yell or scream as loud as possible.
- Do not be afraid to yell for “HELP”.
- If you are being pulled along or dragged, fall to the ground and roll.
- Give bystanders specific instructions to help you. Single someone out and send them for help, e.g. “You in the yellow shirt, call 911.”
- If someone grabs your purse, briefcase, deposit bag or other belongings, DO NOT resist. Throw the item to the ground several feet away from the thief and run in the opposite direction, yelling “help.”
- DO NOT chase a thief.
- Run to the nearest safe place, a safe office, or an open store.
- Call police immediately after the incident.
- If the attack does not warrant calling the police, inform your supervisor



Can workplace violence be eliminated altogether? Probably not, however, based on recognition of the warning signs and utilizing management techniques to de-escalate and report the incidents, the consequences and frequency and total effect will be minimized resulting in a stronger and safer workforce – helping build safe communities.



For more Information, please refer to the Government of Alberta

<http://www.psc.alberta.ca/respectful-workplace-policy.pdf>

<http://www.psc.alberta.ca/respectful-workplace-guidebook.pdf>

Complex Clients

As public service employees, we continuously exhibit the highest standards of conduct and instill confidence and trust amongst the Albertans we proudly serve every day.

Occasionally, however, we are confronted by a small percentage of 'clients' who presents a variety of challenges to the government by deliberately acting inappropriately or aggressively towards our frontline employees. These individuals, deemed **Complex Clients**, if not properly managed, could present a variety of risks and have a detrimental impact on the government, its reputation, values and its employees.



Complex Client - Any person, group or organization who, while interacting with government, seeking services or information, poses a risk to personal safety or intentionally impedes or obstructs the delivery and administration of government services. Complex Clients behaviour can include, but not limited to the following:

- Persistently pursuing complaints on issues that are baseless in fact; have already been addressed; or have no reasonable expectation of a successful resolution.
- Continuously making calls, sending letters, emails, facsimiles or personal visits.
- Inappropriately using previously raised grounds and issues in subsequent complaints.
- Making groundless complaints about government staff and demanding to have them replaced or dismissed.
- Relentlessly pursuing or initiating nuisance complaints with multiple GOA authorities (e.g. Premier, Ministers, Deputy Ministers, and MLAs).
- Refusing to accept a decision, particularly regarding a court matter, and repeatedly arguing a point or otherwise complaining about the decision.
- Alleging department policies and procedures are being applied in a discriminatory or biased fashion without good reason or evidence.
- Maliciously alleging their complaint is being discriminated against on human rights grounds.
- Espousing anti-government ideology (Sovereign Citizens, Freemen of the Land).
- Use of false liens, frivolous lawsuits, unauthentic letters of credit, and other legal-looking documents as a method of harassment or to circumvent processes.
- Conveying peculiar ideas or concepts using legal jargon in an attempt to confuse and coerce government employees to improperly carry-out or alter a Government process.

How to deal with inappropriate conduct or communications

While it is paramount for Albertans to have access to public services, occasionally a client may present a variety of challenges to employees by behaving inappropriately or aggressively. The additional time, effort and resources used to try to manage this complex behaviour can impact an employee's ability to assist other clients.

This information provides Government of Alberta employees with several techniques and procedures for dealing with potential escalating situations and/or inappropriate communication and conduct.



If you read nothing else, read this:

- All clients are to be treated with fairness and respect.
 - In the absence of very good reasons to the contrary, all clients have a right to access public services.
 - All issues raised by clients are to be considered.
 - Unreasonable conduct by a client does not preclude there being a valid issue.
 - The severity of an issue determines the level of resources dedicated to it, not the client's demands or behaviour.
 - Maintaining staff safety and well-being is the most important consideration when dealing with unreasonable clients.
- The decision to change or restrict a client's access to services because of their behaviour can only be made by a manager

Accountability principles for staff

Calm demeanour

Remain calm and maintain control over your emotions and reactions.

Show respect

All complainants, regardless of their conduct, deserve to be treated with respect. Failure to do so can make a difficult situation worse.

Professionalism

Understand that you play an important role in promoting productive and professional interactions with complainants. This includes always maintaining a professional approach—even when complainants are behaving unreasonably.

Dealing with Anger

Try to understand complainant anger: anger is an understandable, and to some degree acceptable, emotion among frustrated and disappointed complainants. The CARP method can help you work constructively with angry clients.

Use the *CARP* Method

- **Control** your interaction with the complainant, including any of your own anger.
- **Acknowledge** the anger and give the complainant an opportunity to 'let off steam'.
- **Re-focus** the conversation to the substantive issues.
- **Problem solve**, find solutions to the issues and problems that you've identified.

What are *your* triggers?

When you have a moment, take time to figure out your triggers. Ask yourself:

- What things do complainants say or do that push my buttons?
- How do I normally react when that happens? Do I respond with confrontation? Do I give in? Do I become dismissive? Am I unaffected?
- Can I respond more constructively in these situations? If so, how?
- What types of customer interactions cause me the most concern? Face-to-face interviews, home visits, or phone calls? Why?
- What can I do to ease that concern?
- What do I perceive as aggressive or violent behaviour?
- How do I deal with such situations?

What to do when you recognize warning signs

- Stop, think and arm yourself with the strategies: by identifying the potential for trouble early on, you have an opportunity to think through the appropriate strategies.
- Check your communication style.
- Make sure you don't act prematurely.
- Set limits and communicate them to the complainant.
- Seek guidance: speak to a colleague or consider sitting down with your supervisor to develop an action plan on how you will respond if the complainant's conduct escalates.
- Assess the risks.
- Keep an open mind and remain positive.

Prevention

- Establish the ground rules.
- Handle the initial interaction successfully.
- Manage complainant expectations.

Managing your expectations

It is not just clients whose expectations can be unrealistic. You may have unrealistic and unreasonable expectations—which can be common for all of us.

The unreasonable client

- Is rude, confrontational, angry, aggressive or unusually frustrated.
- Is overly complementary or manipulative, or makes veiled threats.
- Gives forceful instructions about how complaint should be dealt with and/or by whom.
- Has an unreasonable or unusual sense of entitlement.
- Displays an inability to accept responsibility and blames others.
- Expresses a general dissatisfaction with a person, agency or 'life in general' at the outset and without clear reasons for doing so.
- Appears to have a low anger threshold and very little self-control.
- Is resistant to explanations that counter his/her views.
- Intentionally harasses, intimidates, embarrasses or annoys other people.
- Provides false information.
- Makes excessive demands on resources.

Active Shooter / Assailant Protocol (Get-out-Hide-Fight)

Active shooting/assailant events are exceptionally rare; however, they are becoming a growing phenomenon in schools, public venues and government facilities. While natural disasters such as floods and wildfire may be more prevalent, deadly and costly, the public fear and long-term psychological trauma associated with an active shooter/assailant event outweighs all other calamities.

PROFILE OF AN ACTIVE SHOOTER / ASSAILANT

An Active Shooter or Assailant is an individual actively engaged in killing or attempting to kill people in a confined and populated area. In most cases firearm (s) are used and there is no pattern or method the shooter / assailant uses in the selection of victims. Another thing to consider, an assailant does not necessarily have to employ the use of a firearm. There have been cases where edged weapons, such as knives, were the instruments used to commit mass murder.

Active shooter situations are unpredictable and evolve quickly. Typically, the immediate deployment of law enforcement is required to stop the shooting and mitigate harm to victims.

Because active shooter / assailant situations are often over within 10 to 15 minutes, before law enforcement arrives on the scene, individuals must be prepared both mentally and physically to deal with an active shooter situation.

Best Practices for coping with an active shooter situation

- Be aware of your environment and any possible dangers.
- Take note of the two nearest exits in any facility you visit.
- If you are in an office, stay there and secure the door.

CALL 911 – Only when safe to do so

HOW TO RESPOND WHEN AN ACTIVE SHOOTER IS IN YOUR VICINITY

Quickly determine the most reasonable way to protect your own life. Remember, clients and guests are likely to follow the lead of employees and managers during an active shooter situation.

1. GET-OUT!

If there is an accessible escape path, attempt to evacuate the premises. Be sure to:

- Have an escape route and plan in mind
- Evacuate regardless of whether others agree to follow
- Leave your belongings behind

- Help others escape, if possible
- Prevent individuals from entering an area where the active shooter may be
- Keep your hands visible
- Follow the instructions of police
- Do not attempt to move wounded people
- Call 911 when you are safe

2. HIDE!

If evacuation is not possible, find a place to hide where the active shooter is less likely to find you.

Your hiding place should:

- Be out of the active shooter's view
- Provide protection if shots are fired in your direction (i.e., an office with a closed and locked door)
- Not trap you or restrict your options for movement

To prevent an active shooter from entering your hiding place:

- Lock the door
- Blockade the door with heavy furniture

If the active shooter is nearby:

- Lock the door
- Silence your cell phone/pager
- Turn off any source of noise (i.e. radios, television)
- Hide behind large items (i.e. cabinets, desks)
- Remain quiet

If evacuation and hiding are not possible:

- Remain calm
- Dial 911, if possible, to alert police to the active shooter's location
- If you cannot speak, leave the line open and allow the dispatcher to listen

3. FIGHT!

As a last resort, and only when your life is in imminent danger, attempt to disrupt and or incapacitate the active shooter by:

- Acting as aggressively as possible against him/her
- Throwing items and improvising weapons
- Yelling
- Committing to your actions

HOW TO RESPOND WHEN LAW ENFORCEMENT ARRIVES

Law enforcement's purpose is to stop the active shooter as soon as possible. Officers will proceed directly to the area in which the last shots were heard.

- Officers usually arrive in teams of four (4)
- Officers may wear regular patrol uniforms or external bulletproof vests, Kevlar helmets, and other tactical equipment and will be armed
- Officers may use pepper spray or tear gas to control the situation
- Officers may shout out commands, and may push individuals to the ground for their safety

How to react when law enforcement arrives:

- Remain calm, and follow officers' instructions.
- Put down any items in your hands (i.e., bags, jackets).
- Immediately raise hand and spread fingers.
- Keep hands visible at all times.
- Avoid making quick movements toward officers or holding on to them.
- Avoid pointing, screaming or yelling.
- Do not stop to ask officers for help or direction when evacuating, just proceed in the direction from which officers are entering the premises

Information to provide to law enforcement or 911 operators:

- Location and number of the active shooter(s)
- Physical description of shooter/s
- Number and type of weapons held by the shooter/s
- Number of potential victims at the location

The first officers to arrive to the scene will not stop to help any injured people. Expect rescue teams comprised of additional officers and emergency personnel to follow the initial officers. These rescue teams will treat and remove any injured persons. They may also call upon able-bodied individuals to assist in removing the wounded from the premises.

Once you have reached a safe location or an assembly point, you will likely be held in that area by law enforcement until the situation is under control, and all witnesses have been identified and questioned. Do not leave until law enforcement authorities have instructed you to do so.

Reactions of Managers during an Active Shooter Situation

Employees and customers are likely to follow the lead of managers during an emergency situation. During an emergency, managers should be familiar with the Facility Emergency Response Plan (FERP) and be prepared to:

- Take immediate action.
- Remain calm.
- Lock and barricade doors.
- Evacuate staff and customers via a preplanned evacuation route to a safe area.

Note: While the video below was designed primarily for schools, the concepts can be applied to any facility, including government facilities.

Warning - The video simulates the conditions you might experience during an active shooter event. Some people might find the video disturbing. It might help to view the video with others, such as colleagues, so you can talk about it after viewing it.

<https://www.youtube.com/watch?v=gHNApS-MC18&feature=youtu.be>

Questions about this Active Shooter / Assailant Protocol can be addressed to:
JSG Corporate Security Services - corporate.security@gov.ab.ca

The Alberta Emergency Management Agency (AEMA) has produced a wonderful website to better inform visitors on a number of different risks,

<http://www.aema.alberta.ca/know-the-risks>

RECOGNIZING POTENTIAL WORKPLACE VIOLENCE

An active shooter in your workplace may be a current or former employee, or an acquaintance of a current or former employee. Intuitive managers and co-workers may notice characteristics of potentially violent behavior in an employee. Alert your Human Resources Department if you believe an employee or co-worker is exhibiting potentially violent behavior.

Indicators of Potential Violence by an Employee

Employees typically do not just “snap” but display indicators of potentially violent behavior over time. If these behaviors are recognized, they can often be managed and treated. Potentially violent behaviors by an employee may include one or more of the following (this list of behaviors is not comprehensive, nor is it intended as a mechanism for diagnosing violent tendencies):

- Increased use of alcohol and/or illegal drugs.
- Unexplained increase in absenteeism; vague physical complaints.
- Noticeable decrease in attention to appearance and hygiene.
- Resistance and overreaction to changes in policy and procedures.
- Repeated violations of company policies, problems at home.
- Increased severe mood swings, depression/withdrawal.
- Noticeably unstable, emotional responses.
- Explosive outbursts of anger or rage without provocation.
- Suicidal; comments about “putting things in order.”
- Behavior which is a suspect of paranoia, (“everybody is against me”).
- Escalation of domestic problems into the workplace; ie: financial problems.
- Talk of previous incidents of violence and empathy with those committing it.
- Increase in unsolicited comments about firearms, dangerous weapons and violent crimes.

Telephone Security

Home phone

- Utilize a call display phone.
- Use caution when answering blocked number calls, private number calls, or unknown numbers unless expecting a call from specific individuals.
- Treat with caution any telephone requests to participate in a phone survey of family member or habits.
- Maintain an unlisted and/or unpublished telephone number.
- Consider utilizing the pre-recorded generic answering greeting on your home phone. Avoid utilizing your child's voice or names on your answering message.
- If you do record your own telephone answering message, do not stipulate you are not currently home to accept the call.
- Do not answer your telephone with your name or official title.
- Report all threatening phone calls to law enforcement. Document the content and time of the call.
- Alert any household members to unusual and wrong number calls (if such activity continues, maintain a log and notify law enforcement).
- When in your residence have access to a cordless phone (ensure fully charged) at all times.



Cell phone tips

- Have an accessible and fully charged cell phone (charge routinely).
- On most cell phones you can still call 911 when the phone is locked.
- If you are under immediate risk of harm from another person call 911 and give them your location first. This will assist responding law enforcement to locate you if your call is cut off or you are unable to continue to speak into the phone.
- Using a cell phone in public, WILL cause you to be distracted and therefore substantially decrease your environmental awareness.



Home Security

Be Suspicious

- Be alert to strangers.
- Be alert to anyone requesting access to your residence; check their identification through a peep-hole before allowing entry.
- Write down license numbers of suspicious vehicles; note descriptions of occupants.
- Refuse unordered packages.
- Treat with suspicion any inquiries about the whereabouts or activities of other family members.
- Report all suspicious activity to the local police.
- Never underestimate the violence capabilities, physical capabilities or mindset of anyone.
- Use your senses to help assess the situation and your environment (sight, hearing, smell and touch).
- Trust your instincts, if something doesn't feel right, it probably isn't.



While Away

- Leave the house with a 'lived-in look.' Arrange for driveway/walks to be shoveled in winter and grass cut during summers.
- Stop deliveries or direct them to a neighbor's home.
- Arrange for a trusted person to pick up your mail and flyers.
- Don't leave notes on doors.
- Don't hide keys outside the house (leave with a trusted neighbor).
- Use a timer to turn lights on and off at varying times and locations.
- Leave a radio on (best with a timer).
- Hide valuables.
- Notify a trusted neighbor of your absence.



Answering your door

- Answer your door with it closed and locked. Become accustomed to speaking through the closed door. It's not impolite; it's safe.
- Avoid using chain locks. They present little deterrent to an aggressive person.
- Never open the door to strangers. Verify identification of visitors, sales and service people. Check with the company to see if they sent a representative.
- Should a stranger request to use your phone, do not allow the person to enter your home. Offer to make the call for them but don't unlock your door.
- Don't reveal personal information to anyone on the phone or at your door.

Exterior grounds

- Do not put your name on the outside of your residence or mailbox.
- Install porch light at a height which would discourage bulb removal.
- Install exterior lighting that uses an enclosed light bulb that can't be easily removed and/or install the exterior light at a height which would not permit easy removal of the light bulb.
- Prune vegetation to eliminate hiding places and increase your line of sight when looking out windows.



Entrances and exits, consider

- Solid doors with deadbolt locks.
- One-way peep-holes in doors or a camera / intercom system.
- Security film or security bars on basement windows.
- Ensure patio doors and ground floor windows are equipped with working locking / latching mechanisms (cut-to-size broom handles and hockey sticks laid in the track provide extra security).
- Draw window shades or drapes after dark and don't leave accessible windows open while you sleep.
- Use an electric garage door opener (ensure the opener code on new openers or when purchasing a used residence is changed) and consider not leaving the opener inside your vehicle.

Interior features

- Consider installing a security system and an intercom system.
- When installing a security system consider a second control pad within your bedroom for viewing if the system goes off while you're sleeping.
- Consider choosing a room in your residence (consult a professional) that could be used as a safe room until help arrives.
- The safe room should have a solid core door with dead bolt, security system control panel, fire extinguisher, first-aid kit, phone, flashlight and batteries, and if on the second floor a compact emergency evacuation ladder.

Other desirable features

- A clear view of approaches to your residence.
- More than one access road.
- Off-street parking.
- Have an Evacuation Plan, make it simple and ensure all household members know what to do in an emergency.
- For more information visit [Fire Safety](#).



Mail and Newspaper Safety

- When going out of town, make arrangements with others to have your mail and newspapers secured.
- Never open suspicious packages.
- Report any suspicious packages or mail to the local police immediately.
- Destroy discarded mail – shred any mail with your family's name on it,

Special Precautions for Children

- Instruct children to keep doors and windows locked. Ensure they never tell anyone they are home alone or permit anyone access to the home.
- Teach children how to contact the police or a neighbor in an emergency.
- Know where your children are at all times—morning, noon and night.
- Ensure children never leave home without advising where they will be and who will accompany them.
- Advise Children to:
 - Travel in pairs or groups.
 - Walk along busy streets and avoid isolated areas.
 - Use play areas that are supervised by responsible adults.
 - Refuse automobile rides from strangers and to not accompany anyone on foot.
 - Immediately report to the nearest person of authority (i.e. teacher, police) anyone who attempts to grab, touch or annoy them.
 - Don't put your child's name on personal clothing.



Local law enforcement can provide additional tips and advice on child safety For Domestic Employees and Babysitters

- Conduct a thorough review of references.
- Have they completed a certified babysitting course?
- Inform employees about security responsibilities.
- Instruct them which phone or other means of communication to use in an emergency.
- Do not provide them your home alarm codes.
- Ensure your financial records / statements (bank, credit card statements, pay statements, etc.) are secured so they are not compromised by domestic employees / babysitters.



For More information please visit [Child Safe Canada](https://www.childsafe.ca/)

Internet, Social Media, Identity Theft

Know the Potential Risks of Social Network Exposure of Your Information

Identity Theft

- Identity thieves use an individual's personal information to pretend to be you.
- They use information gathered from public posts, and information in your profile.
- They will steal your mail, credit card statements, utility bills
- They also use information gathered from "social engineering", by "friending" a user and eliciting information through messaging and chats over supposed common interests or common friends.
- They will call you posing as Revenue Canada or a collection agency
- Illegitimate third party Apps may gather information from your private profile that you are not aware of through confusing 'User Agreements' which you may consent to. This information is used to bolster the false identity.
- Attacks may also appear in the form of quizzes, questionnaires, or game links on friend sites that you visit. These sites could potentially capture personal information about you if you play them.
- "Phishing" attempts, the offering of a "lure" to hook you into revealing personal information, such as the "fill out the form to qualify to win an iPod" are also a part of the identity theft fraud toolbox. If it seems to be too good, it probably is so, don't click the link!
- Email may appear to be from the social network itself asking for information, with a link to click. This is another form of Phishing attack. Always check directly with the site by other means to see if you are being "phished."
- "Spear Phishing", highly directed Phishing aimed at a particular individual, where you receive a legitimate looking message which asks you to click a link and enter your login and password on a site usually known to you, but in this case the site will be "spoofed" or falsified. This attempt tries to elicit your information by making you think you have an account problem or a false billing. Don't click the link!
- Using the information gathered, they then can use the synthetic identity to impersonate you. The more information they get, the better the impersonation.

Introduction of Malware

- Malware is malicious software covering a wide range of programs intended to gather information or damage your computer's software or operating system.
- Malware can spread through the social network from contact to contact. The malware appears to come from a trusted contact, which induces people to download it.
- Messages supposedly from a "trusted contact" may include malware links to view a file or video, which result in infection. Always be wary of unknown links.

- A shortened URL on a status update, newsfeed, or blog link may lead the user to download a virus or go to a website that will attempt to download a virus to the user's computer.
- Fake security alerts, with the virus posing as anti-virus, or anti-spyware software, offering to "help you" by clicking the link. Never accept an offer to give you free "anti-virus" help!

Social Engineering Attacks

- Social engineering is the use of information known about a user to elicit additional information from the user.
- "Phishing" and "Spear Fishing" are social engineering methods.
- "Misleading Solicitations" is an attempt to make people feel obligated to join a cause or a group because they receive email from a "friend" who has joined. The intent is to solicit the "registration information" from another user. If you are interested, check with the friend by other means, before signing up.
- "Hijacked Accounts" is the use of compromised legitimate accounts after they are taken over by malware or spyware to defraud other users. The accounts are used to send out spam, malware links, or solicitations to the contacts and friends of the original account.
- A classic example is the solicitation letter from your friend, "stuck in Honduras" and needing a wire transfer to buy a ticket home, after a robbery.

Avoiding Fraudulent Usage of Your Social Networking Information

- Use a strong password (at least eight alpha numeric and 1 capital letter digits), different from the passwords you use to access other sites.
- Never recycle your passwords and change them regularly.
- Use information others do not know about you in your security questions, and never post this information on your public information!
- It is best to not provide a work email to a social network. Consider using a specific new email account only for the social networks. If the account is compromised, your work account will not be compromised.



- Review the privacy policy and how to configure it before you sign up for the account. Make sure you know if there is a change in the privacy policy or terms of service.
- Only provide necessary information you are comfortable with revealing. Leaning to the side of less, is better.
- Never grant access to your contacts or email address book. The network may promise to connect you to people you know who are already on the network, but this exposes your contact list to a whole variety of frauds if it should be compromised. Some networks also use your list, if you do not prohibit them, to solicit your contacts to join.
- Be careful about clicking unknown links in messages from friends on social sites. Links may be fraudulent paths to malware or social engineering attacks. Examine links for oddities, such as misspellings or odd phrasing in the message. If it seems odd, avoid it or check with the friend by other contact means before you “go there”.
- Don’t assume that a message is from who it seems to be from. It is common for hackers to break accounts and compromise contacts lists. If you suspect a fraud, contact your friend by alternate means to see if they are compromised.
- Messages from a social network site will not be asking you to confirm personal information or passwords. Such a message is highly likely to be fraud. Do not click any links and report it to the site.
- Know what information you have posted about yourself. This information is the basis of fraud attacks and help hackers access accounts through the forgotten password approach. Pet names, Mother’s maiden name, first school, favorite hobby, are all common security questions. Think before you post.
- Don’t post vacation plans for the world to know when you are not going to be home! Physical robbery occurs too, not just cyber theft!
- Don’t share all the details of your daily routine. Again, bad actors can be physical criminals, not just cyber criminals. Make sure your children understand what information not to share if they participate in social networking.
- Don’t make it easy for scam artist by posting to the public part of your site your birthdate, age, phone number, and address. This identity information is a gift to potential wrongdoers. If this information is required for registration, restrict it with your privacy settings.
- Type in the name of your social network link or use a personal bookmark when accessing through the internet. Never click a link to your social networking site on someone else’s site. You may be giving your user ID and password information to a hacker.
- Be selective about who you accept as “friends”. Identity thieves may create fake, but attractive profiles, to solicit personal information from you and your site. There is no reward for having the most “friends”! The safest strategy is to reject strangers. If you decide to accept a stranger, limit their access thru your privacy settings. Understand your social network’s privacy settings in detail. They are your best protection against scammers.

- Turn off geo tagging for your pictures so that the world does not know as much about your physical location. Click here for information on disabling [geotagging](#).
- Choose your social network carefully. Know the privacy policy and how to configure it. Find out and understand if the site monitors posted material, and what they do with it. You are providing personal information, so know what they are doing with it.
- Assume everything you put up on the site is permanent and public. The best assumption is that anything you post may become public information.

Social Media and children

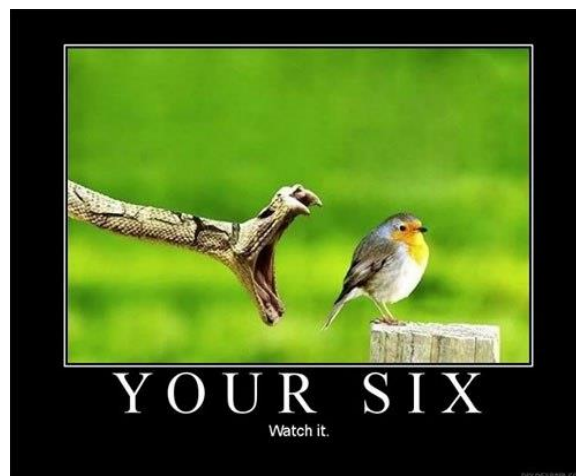
- Discuss the risks of social networking with your children relating to home computing.
- Review their profiles, and postings. Help them configure their sites for proper privacy and to maintain them.
- Make sure they understand what personal information not to post. Make sure they understand what photos not to post, such as embarrassing shots or shots with identifiable location information, such as their house, and including sites away from home such as their school or favorite playground.
- Make sure they know never to meet with someone they have met on line without your knowledge.
- If you are uncomfortable with their use, remove the child's social site by contacting the social network.
- In the event you feel your account has been compromised, notify the social networking site immediately and alert your contacts. Malware may have been installed on your computer. While not a guarantee of safety, scan your computer immediately with up to date Anti-Virus software.



Personal Security Precautions

General

- Avoid high risk areas and occasionally changes routes to avoid predictability.
- Try to be inconspicuous when using public transportation and facilities.
- Understand that public demonstrations can become violent protest.
- Depending on the setting, understand how you dress, conduct, and mannerisms can attract the wrong attention.
- Consider avoiding wearing shirts or caps that identify you or your profession.
- Avoid becoming intoxicated in public places, therefore becoming vulnerable.



Walking / Running / Working out

- Plan your route and avoid short cuts through parks, rear lanes, vacant lots or unlit areas.
- Know where police stations, fire stations or after hour stores are located.
- Continually scan your environment to reassess the situation and avoid areas that are potentially dangerous (make it a habit).
- Avoid walking directly beside building alcoves, doors, and bushes (consider the location, time of day, whether you're alone or not, and presence or not of other persons in the area).
- Remember if it's safer to turn around rather than to proceed ahead.
- Avoid using headphones, (or perhaps only place one earbud in and reduce the volume).
- Vary your routes and try to make sure you are using routes you are familiar with
- Have an escape plan; consider "what would I do if.....happened?"
- Have your cell phone with you with 911 programmed into the speed dial
- Avoid being alone if you can. Get a friend to accompany you. If they can't, let them know your planned route you're taking and time. Call when you arrive.
- Avoid carrying large sums of money or unnecessary valuables Use cash alternatives such as debit cards.
- Protect your bag, purse, knapsack, briefcase when walking; if you don't need it don't take it.
- If someone grabs your purse, backpack or briefcase, do not resist.

Using Automated Teller Machines (ATM)

- Whenever possible, use ATMs in visible and active areas during daylight hours, particularly in areas that are unfamiliar.
- Use ATM operated chartered banks or credit unions. Avoid using generic ATMs that are privately owned.
- If you must use an ATM during inactive periods, consider using a drive-through.
- Avoid using an ATM if the door lock seems defective.
- Be prepared to start your banking as soon as you arrive at the machine.
- Be aware of your surroundings and always make sure that no one has the opportunity to see you entering your pin number or look over your shoulder.
- If danger cues are present or you have a bad feeling, go elsewhere. Danger cues can include someone getting into your personal space, someone who is trying to isolate you from a group, someone who is intoxicated or under the influence, verbal cues or body language.
- Take your transaction receipt with you.

Social / Business Outings

- Considering all circumstances, (time of day, clientele, geographical area etc.) Be cautious when entering a strange or non-familiar bar / lounge / restaurant alone.
- If possible, remain in the company of known people (safety in numbers).
- If the social outing or meeting is at night or in a questionable area, have someone you know/trust walk you to your vehicle.
- If an undesirable contact occurs (i.e. in crowd or on dance floor), immediately disengage and seek friends or authorities.
- Leave the premises whenever you feel uncomfortable (trust your instincts).
- Meet in public, if you're not familiar with the person you are meeting.
- Consider taking your own transportation, particularly if you don't know the person you are meeting, or if the person you are accompanying will not be able to transport you back (Office/residence).
- Do not leave your beverage unattended.
- Have cab money available.
- Consider your proximity to the problem person. Ask yourself, will I be able to react if an attack occurs?
- Be aware of hazards (overcrowding). Identify the possible hazards early and be vigilant.
- Escape routes (for your vehicle, yourselves). How would you get out in an emergency if the way you entered is now unavailable?
- Proximity to exit doors. Could I get to it if an unsafe situation occurred?
- What could you use to defend yourself? Where are they? Can I get to them? Will I be able to use them?
- Movement - Create angles and get out of the line of attack (continually).

Vehicle Security

General

- Avoid the use of “vanity” plates that identify you by name or official position.
- Avoid having your name or official title displayed at your office parking place.
- Obtain a “call police” sign and emergency kit in the event of a break down or emergency (emergency kits for the weather season).
- Clear your vehicle of clutter and avoid leaving enticing items in plain view (e.g. CD's, IPod, loose change, sunglasses, etc....) Avoid leaving your registration and insurance in vehicle.

Vehicle maintenance

- Keep vehicle in good repair.
- Keep gas tank at least 1/2 full at all times.
- Check fluid levels and tire pressure regularly.
- When servicing your vehicle, only leave your ignition key at the garage and not your house keys.



Before Approaching/Entering Your Car

- If possible, look out towards your vehicle prior to exiting the building.
- If exiting your residence, ensure your exterior lights are on to increase your visibility in low /no light hours.
- Have your keys in hand so you do not have to linger before entering.
- Pay attention to who else is in the area.
- Consider having someone you know or trust, accompany you to your vehicle (depending on the time of day, lighting conditions, location of vehicle, and activity in the area). If you're not comfortable continuing to approach your vehicle because of other persons in the area, turn around and go back to seek assistance.
- Utilize reflective surfaces and shadows to detect unseen or concealed persons around the area of your vehicle.
- Avoid appearing to be distracted (i.e. cell phone or head phones).
- On approach to your vehicle look for indicators deserving caution (i.e. broken glass, object from inside the car on the ground, movement in or around the vehicle).
- Listen for other sounds as you approach your vehicle (footsteps).
- View the interior before entering to assure no one is hiding inside.
- Consider not leaving your garage door opener in your vehicle.
- Carry parcels, shopping bags in a shopping cart or in non-dominant hand
- Consider (briefly) activating the panic button on your vehicle as you approach (to startle would be attackers and draw attention of other bystanders in the area).

While in Your Car and Driving

- Always lock your car immediately after entering into and exiting from it.
- Keep the windows closed.
- Know your route and stay on it.
- Never pick up hitchhikers.
- Consider your own safety if you come across a stranded motorist. Call assistance for stranded motorists.

Parking

- Always make a mental note of where you've parked.
- If you are in a parking structure know where the nearest exit is and where you intend to go before you exit your vehicle.
- Try to walk to your vehicle in pairs.
- Park while keeping in mind what the environment will be like when you return. Will it be dark? If so, park near lights.
- Try to park closer to the entrance/exit.
- If possible, reverse your vehicle into the spot for easier exiting.



If You Become Stranded

- Keep doors locked and windows rolled up. If you open your window, only open it to the point of breaking the seal, no further.
- If a stranger offers to help, do not get out of your car. Ask the person to call for assistance or advise them the police are on the way.
- Place a "call police" sign in the window.
- Remember dialing 911 on a cellular phone does not instantly notify police of your location, tell them where you are.
- Know where you are so that emergency services can locate you.



Are You Being Followed?

- Avoid driving home (You do not want this person to know where you live).
- If you suspect that someone is following you, drive to a safe location such as a public space where there are witnesses, help and other ways to notify police.
- Stay in your vehicle and use the horn to draw attention to yourself.
- Go through a drive-through and have them call police.
- Try to obtain the license plate number of the vehicle following you, as well as the make, model, colour and description of the driver.

Road Rage

- How to Avoid
 - Pay attention and drive courteously.
 - Only use a hands free phone while driving.
 - Keep to the right when driving the speed limit.
 - Avoid tailgating, flashing headlights, honking the horn repeatedly or cutting other people off.
 - Use your signals.
 - Leave yourself plenty of time to get where you need to go.
- If you are a Victim of Road Rage
 - Avoid being drawn into an event by another person experiencing road rage.
 - If someone is acting aggressively toward you, do not engage in threatening or insult trading behavior.
 - Avoid leaving the relative safety of your vehicle (Drive away safely if possible).
 - Get a description of the vehicle and occupant(s), including licence plate number and contact the police.



Public Transportation Security

General accepted precautions include, but are not limited to the following:

- While public transit is considered relatively safe, you still need to take certain precautions such as time of day, transit route, number of persons etc.
- Do not stand close to curb or edge of loading ramp of the LRT.
- Don't advertise; conceal expensive jewelry, firmly secure purse (concealed under clothing etc.).
- Maintain a normal pattern of eye contact (when scared or intimidated we often turn away or avoid eye contact thereby providing those around us the impression we are unaware or intimidated).
- Don't let your body language betray you. (When scared or intimidated we tend to instinctively try to make ourselves small and unthreatening. Ask yourself; is the impression that I think I'm giving, the one he/she is actually receiving).
- Vary mode of commercial transportation.
- Use caution in conversations with strangers, avoid giving your name, address or place of employment. Avoid clothing or items that identify you or your profession.
- Try to travel with a companion.
- Carry items in your non-dominant hand, allowing your dominant hand to be free to assist in defending yourself if an unexpected event happens.
- It is important to be aware of your travel patterns/habits. Consider varying or altering your habits if the level of risk should ever increase towards you.

Bus and Light Rail Transport

- Know the schedules and consider sitting near the driver.
- During the evening hours, know the route and where your stop is.
- Have someone meet you at your stop.
- Try to select busy stops.
- Pay attention to anyone getting off at the same stop as you, or while you're walking home, or to your vehicle.
- For More Information <https://www.edmonton.ca/ets/safety-and-security.aspx>



<https://www.calgarytransit.com/getting-around/riding-us/safety-and-security>

Taxi

- Consider varying the taxi companies you use.
- Avoid letting someone you don't know direct you to a specific cab.
- Ensure the face of the driver and the picture on the licence are the same.
- If possible, specify the route you want the taxi to follow.
- Make note of the cab number and the posted operator's identification.



Plane

- Never let your unchecked luggage out of your custody.
- Limit your disclosure of personal information to passengers as they are strangers. Also, remember your conversations are easily heard by others.
- If you have the option of selecting your own seat, select a window seat towards the rear of the aircraft. Disruptions on aircraft normally occur toward the aisle and cockpit.
- For more information visit <https://www.tc.gc.ca/eng/menu.htm>

Acknowledgements

Many stakeholders were consulted or contributed to the material contained in this booklet. Corporate Security Services would like to acknowledge the following entities and their support in keeping us all safe.

- [Alberta Crown Prosecution Services](#)
- [Corporate Human Resources - Occupational Health and Safety](#)
- [Alberta Infrastructure](#)
- [Alberta Emergency Management Agency](#)
- [Service Alberta](#)
- [Edmonton Police Service](#)
- [Calgary Police Service](#)
- [Winnipeg Police Service](#)
- [Peel Regional Police Service](#)
- [State of California Department of Justice](#)
- [United States Marshall Service](#)
- [Canadian Bar Association](#)
- [Pentagon Personal Security Guide](#)
- [Judicial Family Institute](#)

Feedback Invitation

Please assist us in keeping this collaborative handbook relevant and up to date. If you come across any errors, omissions, broken links or have an idea on how to improve this handbook, we would appreciate your feedback at corporate.security@gov.ab.ca