Personal Safety Handbook - Manitoba 2015

Minimizing Risks to Personal Safety for You, Your Family, Friends and Colleagues

THE MANITOBA BAR ASSOCIATION
L'ASSOCIATION DU BARREAU DU MANITOBA
A Branch of the Canadian Bar Association
Une division de l'Association du Barreau canadien

Table of Contents

We are pleased to introduce you to this edition of the *Personal Safety Handbook.* It is a modified version of materials produced by the Ontario and Alberta branches of the Canadian Bar Association. We have adapted the material for Manitobans.

Have you experienced a threat to your personal safety? As lawyers, we should be aware of our personal safety on a day to day basis. An incident of violence occurred against two Manitoba lawyers in July 2015, one of which left a CBA Manitoba branch member with serious physical injuries. The support our members showed during that time was truly inspirational.

What extra steps or precautions can we take to help minimize future threats? Sometimes, the right thing to do is unclear. This handbook is designed to draw your attention to risks and pitfalls in the course of our professional and personal lives. The scenarios presented relate to home and office security, traveling between home and work, identity theft and more. The handbook is designed to help you answer, "What would I do in that situation?"

We would like to thank the volunteer members and staff of the Lawyer Safety Taskforce of the Ontario Bar Association and the Alberta Branch Communications Committee for sharing their information and material. Also, thanks to the Canadian Bar Association British Columbia Branch for their assistance in layout and design of the handbook.

Manitoba Bar Association

Introduction

Potential danger or threats to personal safety are unpleasant topics of conversation to introduce. However, frank discussions, thoughtful consideration and practical measures could ensure the safety of you, your family, staff and property. This handbook is designed to draw your attention to various scenarios many of which are particular to legal professionals.

This handbook attempts to provide ideas to help with these situations.

The following guidelines are suggestions only, and will not cover every possible situation. Individuals are in the best position to assess their own personal circumstances and can adopt any, or none, of the measures suggested in this booklet.

Traveling Between Home and Work

In certain extreme circumstances, your personal safety could be threatened as you travel between home and office or courthouse. Basic precautions can be taken:

- Guard against the establishment of routines by varying times, routes, and modes of travel.
- Be aware of who and what is in your surroundings. Check around your car and in the backseat before getting in.
- Keep your keys in your hands when walking to your vehicle. Remote auto keys have a panic button that will set off your car alarm to attract attention. Your keys can also be used as a weapon in an emergency.
- When driving, habitually ride with seatbelts buckled, doors locked, and windows closed.
- Know locations of safe havens along routes of routine travel.
- If you think that you are being followed, you can test that suspicion by taking a series of right turns and checking if the same person remains behind you.
- If you believe that someone is following you, **do not go home.**
- Proceed immediately to a police facility, or use a cell phone to call the police.
- Note the description of the person (or vehicle) in question and, if possible, get the licence plate number.
- Report the incident to the police immediately! Always ensure your cellular phone is fully charged before going to or leaving from work. If possible, keep a charger and extra charging cable in your car, or keep a portable charger in your briefcase or hand bag.

Vehicles

- Do not use “vanity” plates that identify you by name or profession.
- Do not have your name or position displayed at your office parking space or on parking authority cards.
- Keep your vehicle in good repair. You do not want it to fail when you need it most.
- Keep gas tank at least half full at all times, especially during winter months.
- Park in well-lighted and/or busy areas and park as close to the entrance as possible. If you are leaving work later and your building employs security personnel, ask for an escort to your car.
- Make it a habit to always lock your car.
- Do not leave your car on the street overnight, if possible.
- Never get out without checking for suspicious persons. If in doubt, drive away.
- Leave only the ignition key with parking attendants and service technicians.
- Do not allow entry to the trunk unless you are there to watch.
- Lock away garage door openers.
- Never leave garage doors open or unlocked.
- Use a remote garage door opener if available. Enter and exit your garage in the security of the closed garage.
- Do not leave your personal information unattended in your vehicle, as this will provide your home address. If necessary, lock it in your glove compartment.
- Secure your GPS device or do not record your home address, as this will tell thieves where to find your home.
- If you see a motorist who needs assistance, call the police for them from the nearest telephone (or from your cell phone); do not get out of your car to try to help.

Commercial Buses, Trains and Taxis

- Vary mode of commercial transportation.
- Know where you are going, where you have to transfer and how to get back home.
- Try to use convenient, well-lighted and frequently used stops.
- When boarding the bus, try to choose a seat close to the driver.
- Do not always use the same taxi company.
- Do not let someone you do not know direct you to a specific cab.
- Ensure face of driver and picture on license are the same.
- When riding in a taxi, sit in the backseat.
- Try to travel with a companion.
- If possible, specify the route you want the taxi to follow.

Workplace Security

When at work, it is good practice to be alert to the presence of strangers in the building and on the general premises. If you do not recognize someone as an employee in an area that is usually frequented by employees, or if you notice someone loitering suspiciously, it is appropriate to ask that person what his or her business is in that location. It may be a good idea to offer to escort him or her to the public information desk or reception area. Since staff play a significant part in maintaining the safety of their shared work environment, staff members owe it to each other to be alert at their workplaces.

Should you notice a suspicious car in the parking lot, make note of the license plate number. Specific information makes investigatory follow-up much easier than a general description indicating, for example, a blue Toyota with three males in it.

In Manitoba, all employers, are required to implement an anti-harassment policy under *The Workplace Safety and Health Act*. Employers are also required to carry out a violence assessment and most employers are required to implement a violence protection policy under the same legislation. The *Act* and the regulations contain very detailed requirements as to the specific obligations of employers with respect to preventing workplace harassment and violence. The *Act* and regulations also set out the specific content that such policies are required to contain. We encourage you to review The Act and its regulations to ensure that your workplace has implemented and is maintaining the required policies. Additional information, samples, and resource materials can be located on the SAFE Work Manitoba website at: safemanitoba.com.

The following are some tips from the Winnipeg Police Service's webpage *Safety in the Workplace*:

Sources of Workplace Violence

The main sources of workplace violence can be classified as:

- Robbery / Theft
- Domestic Dispute
- Employer / Employee Directed
- Revenge

Common Types of Violence

- Verbal Abuse
- Disruptive Behaviour
- Threats
- Physical Violence
- Sexual Harassment

Prevention and Management

A formal written policy statement on Workplace Violence should be developed and include sections on the following topics:

- Commitment to Safety
- Code of Conduct
- Management Response Team
- Reporting / Documenting
- Training
- Train Supervisors and employees to recognize warning signs of potentially violent persons
- Educate all staff about workplace violence
- Establish proper security procedures
- Provide counseling and stress debriefing to staff members

Security Checklist

- Provide a receptionist at the entrance to control access at all times
- Escort all visitors in and out of work areas
- Encourage staff to challenge and assist any unaccompanied strangers they encounter in the workplace
- Keep restrooms locked when not occupied
- Have procedures in place for dealing with suspicious mail and packages
- Have a prompt response to incidents of conflict in the workplace
- Develop and use a crisis management plan

Personal Conversations in Criminal Courts or Other Courts

Please keep in mind the nature of the work that you do. Whether prosecuting or defending or simply representing a party in court, such work can routinely involve confrontation and common sense discretion is required at all times.

Court buildings are busy public places attended by all parties to the justice system, including convicted offenders, plaintiffs/applicants, defendants/respondents, their families, witnesses, victims and lawyers, as well as judges and lawyers. The most sensible and appropriate conduct is never to discuss personal matters about yourself, or any other member of the profession within the hearing of any person whom you do not know.

Public Place Security

On an Elevator

- Before getting into an elevator, be aware of those already in the elevator. If someone looks suspicious, do not get in. Wait for the next elevator.
- Once you are in an elevator, always check to see if there is an alarm button, so you can quickly access it, if needed.
- If you are in an elevator and someone suspicious enters after you, get out and take the next elevator.
- If possible, always stand near the control panel. In this manner, if someone in the elevator starts harassing you or threatening you, you can quickly access the buttons (including the alarm button, if available) to allow you to exit at several stops, or to obtain someone's attention.
- It is helpful to be prepared when on an elevator, since you are in a confined space. If you have a hands-on personal protection device such as a whistle, or a small alarm, keep the device in hand so you can readily use it if necessary.
- Never discuss personal or professional matters while on an elevator with persons whom you do not know.

While Walking

- If possible, travel in pairs or with a group.
- Be aware of your surroundings, and do not use unfamiliar shortcuts to save time.
- Plan a safe route and stick to it.
- Stay on busy, well-lighted streets or areas.
- Walk in the middle of the sidewalk.
- Walk facing traffic, so you can see approaching cars.
- Set boundaries and keep a safe distance from strangers in public places or on the street.
- If you believe someone is following you, avoid confined areas; proceed immediately to security or a police facility, or use a cell phone to call the police.
- Be mindful of those around you when discussing personal or professional matters in a public place.
- If you are meeting someone, let them know when they can expect to meet you. That way they will know an issue may have arisen if you don't get to your destination soon after the time provided.

On an Airplane

- Be aware of your surroundings and those sitting beside you.
- If you see something suspicious, advise the flight attendant.
- Be cautious when discussing personal or professional matters while on an airplane with persons whom you do not know.
- Avoid working on confidential matters on an airplane, for example, the person next to you may be, or know someone who is, on the other side of a file. You may wish to invest in an inexpensive privacy screen for your laptop.
- Always ensure you do not leave any belongings on board the plane.

Home Security

Telephones

With the variety of search engines available on the Internet, personal information such as home address and telephone number have become easily available to anyone with on-line access. There are at least a dozen websites that allow an Internet user to locate a phone number and home address at no charge with a click of the mouse. Telephone companies maintain many of these sites themselves. Some of these sites can retrieve, upon entering a name and province, a list of all persons in the province with that name and their respective addresses. Other sites, such as "anyone.com or searchbug.com" have a "reverse listing" feature that allows the user to find an address if the home phone number is typed in.

Precautions You Can Take:

- Ask for an unlisted phone number from your telephone company.
- Consider registering your home number to another name. For example, you may consider using the maiden name of your spouse or of one of your parents. There is no extra fee involved for this service.
- Ask your telephone company about *67 service. It is free for the asking from MTS. This feature blocks your phone number from popping up on someone else's call display. When calling from your home phone, simply key in *67 and wait for the tone before entering the number you are calling. Remember, however, that this service, although free, is not automatic. You must make a specific request of your phone company.
- Post emergency numbers on the telephone.
- Do not answer your telephone with your name or title.
- Report all threatening phone calls to the police immediately.

Family Precautions

Although you may have an unlisted home phone number, your parents or other family members with the same name may continue to be listed. As a general rule, it is probably good practice for family members to refrain from acknowledging to an unknown caller that they are related to a member of the Bar. Individuals calling on legal business would know how to reach you at work and would not need to speak to members of your family.

Surveys

It is not uncommon to be asked to participate in surveys, whether by phone, internet, or mail. Most surveys have a legitimate business purpose and many will offer some kind of thank-you gift for your response. Keep in mind, however, that surveys are simply another form of data bank for your personal information and that you have little control over the use or misuse of the personal details you release. It is up to you to decide if that free magazine subscription is worth the dissemination of your household income information to persons unknown.

Your Home Address

Many retail businesses routinely ask you for your home address when you make a purchase. That information can be a useful retail tool to identify customers for catalogue or promotional mailings. You have the option to decline to provide the personal details requested. As with surveys, this information goes into a data bank. It is up to you to decide if you wish to participate.

Securing Your Home:

- Restrict the possession of house keys.
- Change locks if keys are lost or stolen and when moving into a previously occupied residence.
- Consider use of biometric locks (fingerprint scanners).
- Lock all entrances at night, including the garage. Keep the house locked, even if you are home.
- If you have an auto remote key for your car, keep it by your bedside at night. If you suspect someone is trying to break into your home, activate your car's panic button to set off the alarm in the driveway or garage (be sure to test that it is in range).
- Install alarm and intercom systems.
- Secure your residence with high quality locks, secure sliding glass doors and reinforce the wood frame around door locks. This security measure can usually be implemented at relatively little cost.
- Install one-way peep-holes in doors.
- Install bars and locks on skylights.
- Consider keeping your cell phone in the bedroom while sleeping. This can be a vital, immediate means of communication if your residence phone is disabled during the night.
- Do not put your name on the outside of your residence or mailbox.
- Control vegetation to eliminate hiding places.

- It may be useful to install motion sensors. Consider upgrading your outside lighting and installing it high above ground to deter tampering.
- Maintain several fire extinguishers in your home.
- Establish and practice a fire safety plan.
- If your residence has a garage, consider securing the garage door from the inside at night, especially when you are on vacation. A simple inexpensive bolt placed in the door track will prevent it from being opened. Remember that the cheap outside lock is easily defeated.
- If your home has a direct entry/exit door from the garage into your home then the security of this door should be considered as important as that of the front and back doors. Ensure that the garage entry door is secured with a good deadbolt lock.
- Be alert to peddlers and strangers.
- It is not a good idea to allow repair personnel into your home if the visit was not planned in advance. Local public utility or gas employees normally carry photo ID when they respond to repair calls. Check their ID. You should permit entrance only if you are confident of their identity.
- If you live in an apartment building or condominium, your parking spot should not display your apartment or unit number. Rather, it should have another number assigned by building management that only you and building management know.
- If you live in an apartment building or condominium, you may request your building manager to delete your name from the residents' list in the lobby.
- Treat with suspicion any inquiries about the whereabouts or activities of other family members.
- Be mindful about posting detailed pictures of the inside or outside of your home on social media accounts.

Mail

- Avoid putting a "stop mail" notice at the post office while you are away from home on vacation or business trips. Such action simply broadcasts that a particular home is vacant. Have a trusted neighbour or family member take responsibility for your mail each day. Even if your mail goes to a postal super box, arrange to have it picked up. A mailbox that is emptied each day gives the impression that the residence is occupied.
- Refuse unordered packages.

- Watch for suspicious packages or mail with these characteristics:
    - An unusual or unknown place of origin, such as a foreign country.
    - No return address or a fictitious return address.
    - Badly typed or written words.
    - The package is addressed to a title only (e.g. “President” or “Resident” or “Counsel”)
    - An excessive amount of postage.
    - Abnormal or unusual size.
    - Rigid or bulky package. Lopsided or uneven packages.
    - Oily stain on the package, discolourization or crystallization on the packaging.
    - Unusual endorsements or restrictive markings (e.g. “Personal”)
    - Wires or strings protruding from/attached to an item.
    - Incorrect spelling on a package label.
    - Differing return address and postmark.
    - Peculiar odour. (Many explosives smell like shoe polish, almonds or spices.)
    - Unusual heaviness or lightness.
    - Uneven balance or shape.
    - Springiness in the top, bottom, or sides.
- Never cut tape, strings, or other wrappings on a suspected package; never immerse a suspected letter or package in water. Either of these actions could cause an explosive device to detonate.
- Never touch or move a suspicious package or letter.
- Report any suspicious packages or mail to the police immediately.

Canada Post recommends the following precautions if you receive a suspicious package:
1. Immediately advise local emergency services of the situation.
2. Do not handle, shape, smell or taste the suspicious article.
3. Isolate the article and evacuate the immediate vicinity.
4. Anyone who has handled the article should immediately wash their hands with soap and water.

Office Files & Documents:

- Never leave work files, laptops, tablets or other information in a visible location in your vehicle. Use your trunk for safe storage.
- When working on files at home, shred all drafts/duplicates.

Bills and Receipts

Old bills, invoices and receipts contain a great deal of personal and financial information that, if misused, can result in your becoming a victim of identity theft and fraud.

Much of today's junk mail consists of "pre-approved" credit card applications that already bear your pre-printed name and address on the form. It is conceivable that another party could apply for a credit card in your name.

A relatively inexpensive paper shredder can be purchased from most business supply retailers.

- Shred old bills, cheques, credit card invoices, cards and merchandise receipts before disposing of them in the garbage or recycling bin.
- Shred unsolicited mail offers and old subscription magazines.

Personal Cheques

If you still write personal cheques, consider arranging with your bank for your cheques to display only your name and not your home address. Most bank and trust companies will offer this at no extra charge. You may be required to pick up the cheques from your bank branch since they cannot be mailed.

Since cheques routinely display the name of the bank and the account number, it is wise to keep to a minimum the amount of personal information available on that document.

Domestic Employees

- Conduct a thorough review of references and a police criminal record check.
- Inform employees about security responsibilities.
- Instruct employees as to which phone or other means of communication to use in an emergency.

Vacation

When going on vacation away from home, do not broadcast the fact on your voicemail system at work or home. At the office, a message that advises callers you are not available and refers them to another person for assistance is sufficient.

A similar message on your home voicemail advising callers that you are not available is likewise appropriate. Your colleagues, friends, and other family members should not confirm to callers that you are away from home.

Be careful in making social media posts about being on vacation.

Familiarize your family with the necessary protective measures and techniques in this handbook. Review these measures periodically. Ensure that everyone in the family knows what to do in an emergency. And, when anything suspicious occurs that just might suggest a threat to your safety, call the police immediately. Let them decide whether or not "it's nothing to worry about".

Fraud and Identity Theft

Fraud has become a significant problem. You may be a victim of fraud personally or professionally.

As a victim of fraud, there are many possible consequences: repairing credit ratings, reclaiming identity, mental distress, property, time and economic loss, defence costs and interruption of work or business. Fraud has become commonplace.

Prevention

- Always store cards and documents, such as birth certificates, social insurance numbers and passports, containing personal information in a secure place, and shred them after they expire.
- Review the balances on your statements from banks, credit cards and companies regularly. Report any discrepancies, however minor, right away. Fraudsters often steal in small amounts from many cards to evade detection.
- Once a year, get a copy of your credit report from the two national credit reporting agencies, Equifax Canada and TransUnion Canada (See Appendix for contact information). The report tells you what information the bureau has about your credit history, financial information, any judgments, collection activity and who has asked for your information.
- If your bills do not arrive, or you applied for a new credit card that has not arrived on time, call the credit grantor immediately.
- If you are going to be away from home, ask a trusted neighbour to pick up your mail and newspapers.
- Consider whether identity theft insurance coverage may be available to you. For example, some title insurers offer this as an add-on to a residential title insurance policy.

Online Theft

- Fake or "spoof" websites are designed to trick consumers and collect their personal information. Be cautious when clicking on a link or an unknown website or unfamiliar e-mail. The link may take you to a fraudulent site.
- Be wary of computer start-up software that asks for registration information.
- Never share your passwords.
- Do not use e-mail to send personal information.
- Discourage harvesting of your e-mail address – think about creating “disposable” e-mail addresses for online purchases, mask your address or use a unique e-mail address.
- Beware of Internet promotions that ask for personal information. Identity thieves may use phony offers to get you to give them your information.
- After completing any sort of financial transaction online, make sure you sign out of the website and clear your internet file/cache. Most financial institutions provide instructions on how to clear the caches under their “security” section.
- Do not give a credit card number or other identification information to a company that doesn't provide its name, business address, telephone number and e-mail address.

- Before giving your credit card number or other financial information to a business, make sure that their website is protected and secured. Look for a lock symbol located somewhere on the browser or make sure the URL begins with "https://"
- Chain letters and phony investment schemes try to win your confidence with false promises of incredible returns – they are interested in obtaining your personal and/ or credit information. There are many types of investment frauds and scams. Many are convincing and look very real.
- Teach children about not sharing overly identifying personal information on social media. Help them learn that any information they exchange on the internet is not private.
- Look into encryption, firewalls and virus protection for your computer.
- Identity thieves can take simple information such as your birthday or your pet's name as clues to common passwords and steal your identity.
- Understand that information exchanged on social network sites is not private.

Securing Your Laptop

Do you regularly travel to the U.S. on business? If you take confidential information of any kind with you, take heed: a new policy allows agents of the U.S. Customs and Border Patrol (CBP) to search and confiscate computers, phones, personal digital assistants, cameras, digital music players and other data-storing devices. Operating under the new U.S. Policy Regarding Border Search of Information, agents have also downloaded the contents of entire computer hard drives and other storage media for later review.

Below is an excerpted list from *How to Secure Your Laptop Before Crossing the Border* by Luigi Bennetton, on how you can shield sensitive information, like that protected by solicitor-client privilege, when crossing the border. A complete copy of the article and links to other resources can be found at www.cba.org/CBA/practicelink/tayp/laptopborder.aspx.

Each one comes with caveats, the most important of which is that there are no guarantees. You should consult an IT security expert to help you choose the best options for your needs.

- Travel with a "bare" computer. The CBP cannot read what a computer does not contain. That is why certain companies give their employees "forensically clean" computers for travel. These computers contain the operating system, required applications, and little or no data. Once at their destinations, employees work with data stored on company servers via secure virtual private network (VPN). (Secure connections are a must since, under certain circumstances, U.S. law permits interception of e-mail and remote server connections.) Employees may download files to their computers, upload the results of their work to company servers and "forensically clean" their computers before traveling again.

- Turn off your computer. If you must bring data on your computer, turn it off five minutes prior to reaching customs. While running, computers store unencrypted information in random access memory (RAM). If you walk through customs with a computer in sleep mode, the RAM shows what you were working on
- Back up your data. Should border agents confiscate your computer, they will not stop your ability to work billable hours – as long as you left a copy of your data in a safe place, such as another hard drive or your company's servers, and you can quickly recover all that data (documents, calendars, e-mail and so forth).
- Partition and encrypt your entire hard drive. Hard drive partitioning, like encryption, is a common IT practice that enables people to use a hard drive as though it were two or more drives. These partitions can be encrypted using different passwords. Privacy application: Encryption and partitioning, when combined, allow a traveler to decrypt a partition that contains "safe" data for border agents to inspect. Agents might not know to look for other partitions if the partitioning tool hides them – a tactic known as steganography. Why the entire hard drive? Certain programs can record information outside of encrypted areas without a user's knowledge.
- Protect FireWire ports. FireWire is a type of data port that allows for faster data transfers than are possible via USB. The CBP can quickly copy an entire hard drive via FireWire. Macs let their owners block this option by setting an Open Firmware Password. Consult your IT provider for advice on how to protect your FireWire port.
- Store data on small devices. Camera memory cards and USB memory keys can store huge amounts of data. Since they are small, you can carry them inconspicuously. Also because they are small, they are easily lost, and just as easily confiscated by border agents if found, so use strong encryption on these devices as well.
- Protect phones and other electronic devices. Phone records, text messages, emails, documents – today's phones carry amazing amounts of information. Keep the device as "clean" as possible if you think it might be confiscated. Also, enable any password locking and encryption tools, if available. Another possible solution: certain smartphones can be "wiped clean" remotely when they are reported lost. Every one allows users to synchronize the data on them onto their computers so that they can quickly put the data onto a replacement unit should the need arise.
- Clean your laptop when returned. Border agents might even return confiscated laptops with a little something extra: spyware that tracks the owner's computer activity and sends log files back to "Big Brother." "Fedware" may be invisible to onboard spyware scanners, so the first thing to do when you get your laptop back is to boot it using an external drive and scan the onboard drive for anything that should not be there.

If You Are A Victim

If you think that you have been a victim of identity theft, there are steps you should take immediately to minimize damage and help prevent further fraud or theft:

Step One
Contact each financial institution, credit card issuer or other company that provided the identity thief with unauthorized credit, money, goods or services.

Step Two
Contact Canada's two national credit reporting agencies, TransUnion Canada and Equifax Canada (numbers contained in the Appendix).

There are two things you should do when you call:

- Ask each agency to send you a copy of your credit report.
- Discuss whether you should have a fraud alert placed on your file, asking that creditors call you before opening any new accounts or changing your existing accounts.

The credit report may reveal whether there are other companies where the identity thief has opened accounts or incurred debt in your name.

Step Three
Report the incident to your local police department and ask them to take a report. If a police report is available, include it in all correspondence with financial institutions, credit issuers, credit reporting agencies and other companies.

Step Four
Report the incident to the Canadian Anti-Fraud Centre (CAFC) toll free at 1-888-495-8501. CAFC gathers information and intelligence about identity theft, and provides advice and assistance to victims. It can also be a useful source of information about new fraud schemes. CAFC's website can be located at: www.antifraudcentre-centreantifraude.ca/index-eng.htm

Step Five
If your credit cards or government-issued documents (such as driver's licence, birth certificate or passport) have been lost or stolen, notify the issuing authority immediately to have the document cancelled and a new one issued.
Note: Keep a record of your actions, even after the case has been resolved. Errors can reappear on your credit reports or your information can be re-circulated. If this happens, you'll be glad you kept your files.

It's Up to You to Take the First Step!

Understanding and Reacting to Various Threats

911

Seconds count in an emergency! When you have an emergency, dial 911. When police, fire, or medical emergencies occur, 911 can help save precious time. Your call is answered by a trained emergency call taker who will provide you with the assistance you require. You can also dial 911 from your cellular phone. The call is toll free. If you do not have 911 service in your area or if it is not an emergency, consult your local directory for options and have these numbers readily accessible to you, your family and staff.

When you make a 911 call from a wireless/cellular phone, communicators DO NOT receive the phone number and address from where the call originated. If you provide your cellular phone number to the 911 communicator, the communicator will be able to reach you in case the call is disconnected, which often happens with cellular calls. Make sure you have the number written down in an easy to find location before you need to call 911. It is a good habit to identify beforehand any nearby exits and "safe havens" such as police, fire stations (some are not manned 24 hours), 24-hour stores or gas stations, friends, etc. where you can get assistance and shelter if physically threatened.

If you think the threat targets your children, instruct them to be vigilant and to react as they have been instructed by you, or at school, concerning "suspicious behaviour" by strangers. Identify two to four "safe havens" where they can go for assistance if they feel threatened. For young children, laminate a card that you attach to their backpack with all necessary emergency contact numbers and addresses. Familiarize yourself and your children with the Block Parent® Program, a network of concerned citizens who provide safe homes in our communities for anyone, particularly children and seniors, who find themselves in a frightening or dangerous situation and need immediate help. Block Parent® volunteers are trained and screened by a multi-step process, which includes criminal background checks on a regular basis.

Identifying and Dealing with Potentially Violent Persons

The Winnipeg Police Service, on its webpage Safety in the Workplace, provides the following guidelines in terms of identifying and dealing with potentially violent persons:

WARNING SIGNS

Be aware of the following warning signs of a potentially violent person:

- Resists change
- Sullen, angry and/or depressed
- Identifies with or praises acts of workplace violence
- Recently collected or obtained a weapon
- Uses threats, intimidation and manipulation towards others
- Paranoid - thinking others are out to get them
- Over-reacts to criticism
- Blames other people for their own mistakes
- Has had recent police encounters
- Has a history of assault
- Other persons are afraid of, or apprehensive about this person

STAGES OF AGGRESSION

- Person becomes anxious or on edge
- Displays negative attitude and/or behaviour (refusal to cooperate and questioning)
- Verbal - physical release
- Calms down

RESPONSES TO THESE STAGES

- Show support and empathy for them
- Be firm and set limits
- Escape and get assistance
- If future contact is expected, set firm ground rules

BE AWARE OF NON-VERBALS

- Watch out for non-verbal clues that someone is becoming violent:
- Personal space
- Body language (clenching / unclenching fists)
- Facial expressions
- Tone of voice

TYPES OF THREATS

- Direct - "I'm going to kill you"
- Conditional - "If you report me - you'll regret it"
- Veiled - "Be careful going home tonight, I know where you live"

DEALING WITH THREATS

DO:

- Stay calm
- Assess the situation
- Agree with them
- Report and document immediately

DON'T:

- Panic
- Beg or plead
- Argue or escalate the situation
- Minimize the threat
- Fail to report the incident

RESPONDING TO INCIDENTS

The following are critical management steps:

- Call 911 immediately
- Secure and control the area
- Account for everyone in the area
- Ensure their safety
- Evacuate if required
- Assist emergency crews
- Have floor plans available if required
- Have employee lists available
- Have all departmental phone numbers on hand
- Provide suspect information if relevant

WORKING ALONE

If you work shifts or work into the evening alone, take precautions to reduce your vulnerability and protect yourself:

- Whenever possible, try to avoid working alone.
- If you are required to work alone, develop a check-in system with a friend or family member and let them know you are okay. Give them instructions on what to do if you do not check-in on time (i.e., calling the police or a manager).
- If you work in an office, make sure all doors and windows are locked. Turn on several lights to make it appear the building is occupied.
- Let someone know when you are leaving, the route you will be taking and when you are expected to arrive home.
- If possible, have someone escort you to your vehicle. Try to park your vehicle in a well-lighted location close to the door.
- The Workplace Safety and Health Act and its regulations impose obligations on employers whose employees work alone. You should consult the Act and regulations to ensure that such safety precautions are implemented and maintained.

How to React to Specific Circumstances

E-Mail/Cyber Threat

Cyberspace, with its world-wide reach and the possibility of anonymity, is an appealing medium for would-be aggressors.

Electronic evidence requires special handling. When an e-mail or cyberspace threat has been made against you, or a member of your family, do not attempt to solve it by yourself. Immediately notify the appropriate authorities.

Mail or Courier-bound Threats

Mail or courier-delivered threats usually consist of a threatening message or the presence of a possible harmful component or substance. If you suspect such a threat, do not handle the envelope or package further. Let trained personnel properly handle and dispose of it.

Telephone Threats

Try to record the call if the telephone is equipped with a recording system (e.g. an answering machine or portable recorder/dicta-phone). If equipped with caller identification, note the information displayed.

- Remain calm. Telephone threats are usually meant to disrupt an organization's operation, or instill fear. If the call is genuine, the caller should be willing to give a minimal amount of verifiable information to establish the threat is credible.
- Inform the caller that in order to validate his/her threat, some verifiable information is required. Ask:
    - Who is the intended target?
    - What is the message/threat?
- If it is a bomb threat, ask:
    - Where is the device?
    - What does it look like?
    - When will it explode?
    - Who are you?
    - Why are you doing this?
- Document the information and contact the appropriate authorities immediately.

Being followed…

On foot

If you suspect or notice that someone is following you, do not confront the person. Unless physical danger is imminent, do not attempt to lose or outrun the person.

Discreetly observe their behaviour:

- Do you know the person or persons?
- Do they appear to communicate with someone else or each other?
- If so, how (concealed radio, cell phone, gestures)?
- Is it possible that the surveillance is directed at someone else* (See note next page).
- Make a mental note of the person's features (sex, age, height, hair, clothing, etc.).
- Do they make menacing gestures or other threats?

If possible stay in or near a crowd. If you feel threatened, discreetly and calmly ask a passer-by or someone else to escort you to a safe location.

When you have reached a safe location, document the event and seek appropriate assistance.

In a Vehicle

If you suspect or notice that someone is following you, do not confront the follower. Unless physical danger is imminent, do not attempt to lose or out-drive the other vehicle.

Discreetly observe their behaviour:

- Do you know the persons or person?
- Do they appear to communicate with someone else or each other?
- If so, how (concealed radio, cell phone, gestures, etc.)?
- Is it possible that the surveillance is directed at someone else* (see note next page)?
- Make a mental note of the person's features (sex, age, height, hair, clothing etc.) and of the vehicle (colour, make, license plate number etc.).
- Do they make menacing gestures or other threats?

If you feel threatened, stay in your vehicle and ensure your doors are locked. If you have a cell phone use it to contact the police. Drive safely towards a secure location. If you encounter an emergency vehicle (police, fire, ambulance) signal for assistance by flashing your high beams, continuously honking your horn or turning the vehicle around to follow.

When you have reached a secure location, document the incident and seek appropriate assistance.

*NOTE: Public and private investigators, or police, may legally follow a person, either as the direct or indirect subject of an ongoing investigation. An indirect subject is related in some way to the subject of an investigation. The object of the surveillance is to establish his/her identity and relationship with the subject. You may, therefore, find yourself the indirect subject of an ongoing investigation. If you suspect you are under surveillance, document the incident and report it as soon as possible to the proper authorities. Additionally, some stores are staffed with security and/or loss prevention personnel who routinely follow customers in order to detect and deter shoplifting.

Appendix

It Just Happened…A Guide to Evaluating the Risks and Impacts of Threats Against Department of Justice Employees
Department of Justice Canada

Personal Security Handbook …How You and Your Family Can Minimize Risks to Personal Safety
United States Marshals Service
www.ncjrs.gov/pdffiles1/Digitization/124321NCJRS.pdf

Intuitive Security for Women
By Lloyd Vaughan and Luke Chao

Equifax Canada®
1 800 465 7166
www.equifax.ca

TransUnion Canada®
1 800 663 9980
www.transunion.ca

How to Secure Your Laptop Before Crossing the Border
Luigi Bennetton
Originally published in 2008 on CBA PracticeLink
www.cba.org/CBA/practicelink/tayp/laptopborder.aspx

Suspicious Mail Alert
Canada Post
www.canadapost.ca/cpo/mc/assets/pdf/aboutus/suspiciousmailposter_en.pdf

Winnipeg Police Service
Safety in the Workplace
winnipeg.ca/police/TakeAction/safety_workplace.stm

THE MANITOBA BAR ASSOCIATION
L'ASSOCIATION DU BARREAU DU MANITOBA
A Branch of the Canadian Bar Association
Une division de l'Association du Barreau canadien