# 2019

# Fraud Prevention & Safety Handbook

for Individuals



The Fraud Prevention & Safety Handbook for Individuals is Presented by:

















310 University Park Drive Regina, SK S4V 0Y8

Tel: (306)585-2202 Fax: (306)585-2280

ralph.goodale@parl.gc.ca

ralphgoodale.ca



House of Commons Chambre des communes



#### **SAFE & SECURE**

I want to congratulate Saskatchewan Seniors Mechanism and all the partners who have come together to produce this very useful handbook on safety and fraud prevention.

This is a valuable source of information and support for the public generally, but especially for seniors.

As Canada's Minister of Public Safety and Emergency Preparedness, I have two major policy objectives:

- \* first, to ensure that all federal departments and agencies are working effectively with their provincial and municipal counterparts to keep Canadians safe;
- \* and secondly, but of equal importance, to safeguard the precious rights and freedoms of Canadians and the diverse, open, inclusive and democratic character of our society.

All our efforts need to be undertaken in close partnership with the public. That's why I welcome this handbook which makes valuable information and local contacts readily available, while encouraging a healthy level of care and vigilance when dealing with other people - in person, over the phone or on the internet.

This handbook will help to make us all safer. My thanks to all the contributors.

Sincerely,

Raiph Goodale, MP (Regina-Wascana)

Minister of Public Safety & Emergency Preparedness

# **CONTENT**

#### 4 INTRODUCTION

#### 5 SCAMS & FRAUD PREVENTION

- 6 Scam and Fraud Definitions
- 7 Debunking 'Old' Myths About Scam Victims
- 8 Scams and Fraud Contact Methods
- 9 Top 10 Scams Campaign
- 9 BBB's Anti-Scam Pledge
- 10 Advance Fee Scams
- 11 Charity & Donation Scams
- 12 Credit Repair and Debt Relief Scams
- 13 Door-Knocker Scams
- 14 Employment Scams
- 15 Fake Cheque/Overpayment Scams
- 16 Home Improvement/Contractor Scams
- 17 Investment Scams
- 18 Medical Cures Fraud & False Benefit Claims
- 19 Online Purchase Scams
- 20 Online Romance Scams
- 21 Phishing Scams
- 22 Phone Call Scams
- 23 Puppy/Pet Scams
- 24 Sweepstakes, Lottery & Prize Scams
- 25 Tech Support Scams
- 26 Travel & Vacation Scams

# **CONTENT**

#### 27 PERSONAL INFORMATION & IDENTITY THEFT

- 28 Signs Your Identity Is Being Used
- 28 How Con Artists Get Information on Potential Victims
- 30 How to Minimise Your Risk of Identity Theft
- 31 What to Do If You Suspect Someone Has Stolen Your Identity/SIN/Other Documents
- 32 What You Can Do About Identity Theft

#### 33 CYBER & EMAIL SECURITY

- 34 What Is the Difference Between Viruses, Trojans, Worms and Other Malware?
- 35 What You Can Do to Keep Your Computer Cyber Secure
- 35 How to Create a Strong Password
- 36 Top 10 Spam Email Subject Lines
- 37 Tips for Spotting a Bad Email

#### 39 PERSONAL & HOME SAFETY

- 40 What You Can Do About Abuse
- 41 Take Care of Your Physical and Mental Wellbeing
- 41 Home Safety
- 42 Home Fall Prevention Checklist

#### 47 ADDITIONAL RESOURCES & CONTACTS

# Introduction

Thank You for Picking Up a Copy of the Fraud Prevention & Safety Handbook for Individuals

The Fraud Prevention & Safety Handbook for Individuals is a resource especially intended for older adults, designed to help people be safe in their homes and communities. It has been created through the collaboration of the Saskatchewan Seniors Mechanism, Better Business Bureau of Saskatchewan, Government of Saskatchewan Financial and Consumer Affairs Authority, Regina Crime Stoppers, Saskatchewan Crime Stoppers, Regina City Police, Royal Canadian Mounted Police and the Saskatchewan Safety Council. Raising awareness of fraud and scams is the main focus of this resource, but it also includes other safety information we hope you will find useful.

#### **How To Use This Handbook**

Read through the information and make yourself better informed. Then keep it handy as a reference guide.

If you are part of a seniors' group or any other group that gets together for meetings or coffee, you may like to choose one or two items for the topic of a short discussion each time you meet. This helps share the information and makes you and others aware of ways to avoid fraud and scams, address issues of older adult abuse, and maintain your personal safety.

You may wish to share your copy of this handbook with someone else or order it for them. You might want to talk to your family members or friends about the areas covered in this resource. If those closest to you are also aware of the topics covered here, they can help you be safer and they may also learn things to keep them safer as well.

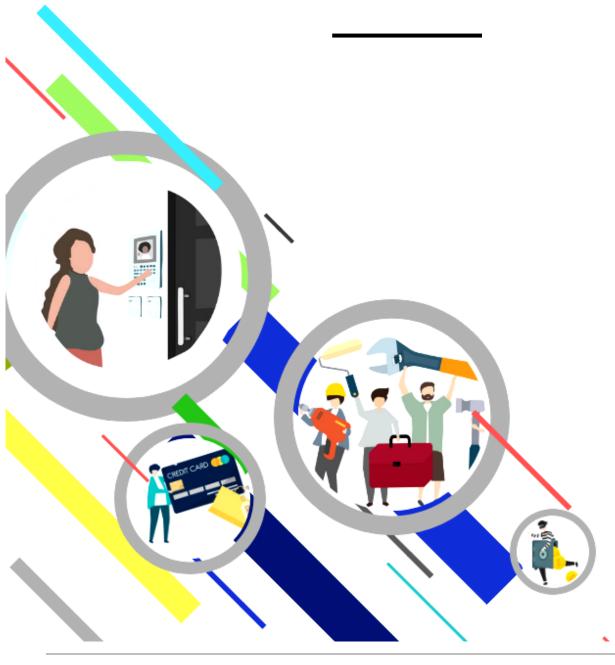
While this resource is focused on keeping older adults safe, it is something everyone can make use of. Older adults are no more likely to fall for scams than anyone else of any other age, just that the type of scam/fraud that is successful changes with life experience.

We hope you find this resource helpful and that it keeps you and those around you safe in your home and in your community.

For print copies of this Handbook, please contact Saskatchewan Seniors Mechanism at:

#112-2001 Cornwall Street Regina, SK S4P 3X9 or phone (306) 359-9956

# SCAMS & FRAUD PREVENTION



# Let's Talk Scams and Fraud

Awareness Is Your Best Protection Against Being a Victim of Scam and Fraud

Scams come in a variety of forms, and classifying them is an ongoing challenge. For the purpose of this handbook, the scams and types of fraud listed in the following pages are those considered the riskiest to older adults and the most active scams in our communities today.

# **DEFINITION: SCAMS**

Scams are questionably legal acts. A scam occurs when a con artist takes money from someone but technically does not break the law when he/she does so.

**Example:** You may have purchased a brooch that was advertised as a "yellow gold" brooch and you may have paid a fairly steep price for it thinking it was actually gold. Once you get the "gold" brooch home, you realize it is not gold at all. You may have been misled by the term (yellow gold); however, technically, the con artist is only guilty of overcharging you for the brooch.



### DEFINITION: FRAUD

Fraud is a clearly illegal act. Fraud occurs when a con artist uses deception to make a profit or to take your money. They pretend to be someone they are not or say they will do something they don't do.

**Example:** A con artist from out of town may sell you a puppy over the Internet. He/she will give you every indication that the puppy will be sent to you once you make payment. You never see the puppy. In fact, the con artist likely never owned the puppy in the first place and was simply using photos stolen from other websites to entice you to buy.

# **Debunking 'Old' Myths About Scam Victims**

Why Seniors Are Not More Likely to Be Victims of Scams and Fraud

In 2017, Better Business Bureau (BBB) released a research report on the top riskiest types of scams and fraud facing consumers of all ages across North America, using information collected through its ScamTracker® online scam reporting tool.

The data showed a marked trend toward decreased susceptibility with increasing age. About 38 percent of individuals who provided age information when reporting to BBB ScamTracker® were 55 years of age or older, yet this group was far less likely to report a financial loss than the younger age groups.

Younger adults (identified as the Millennial generation and younger) were far more likely to fall for scams that used online means of contact (e.g., website, email, Internet messaging, online classifieds, etc.).

The truth is there is a scam for everyone. As we gain more life experiences, we become better at recognizing and avoiding some scams but continue to be susceptible to others. By acknowledging which scams might be targeting us, and educating ourselves on common scam tactics and red flags, the better equipped we are to keep ourselves and loved ones safe.

Top 3 Riskiest Scams by Age Range	2017 BBB Scam Tracker Annual Report
-----------------------------------	-------------------------------------

AGE RANGE	TOP 3 MOST RISKY SCAM TYPES		
	1	2	3
18 - 24	Fake Cheque/Money Order	Online Purchase	Employment
25 - 34	Employment	Online Purchase	Advanced Fee Loan
35 - 44	Online Purchase	Fake Cheque/Money Order	Advanced Fee Loan
45 - 54	Investment	Online Purchase	Employment
55 - 64	Romance	Investment	Employment
65+	Tech Support	Family/Friend Emergency	Investment

If you are interested in reading the full Better Business Bureau research report on perceived victimhood and the latest Scam Tracker Risk Report, you can find them online here:

Breaking the Invulnerability Illusion—bbb.org/truthaboutscams 2017 Scam Tracker Risk Report—bbb.org/bbbscamtrackerriskreport

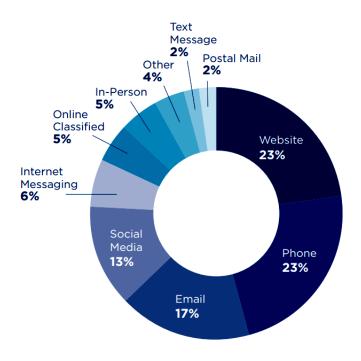
# **Scams and Fraud Contact Methods**

Awareness Is Your Best Protection Against Being a Victim of Scam and Fraud

Scammers and fraudsters exploit the full range of communication channels to make contact with their targets, and quickly adopt new or popular contact methods if it might mean they can be more successful while keeping their anonymity.

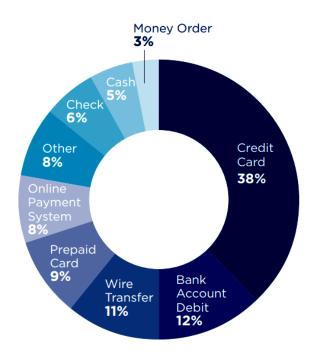
#### **MEANS OF CONTACT**

In 2017, contact through websites matched the phone as the top means of contact for scams with actual loss of money. Scams delivered by all of the various forms of online delivery (i.e., email, website, social media, online classifieds, etc.) account for approximately 67 percent of all reports of monetary loss.



#### **MEANS OF PAYMENT**

Scammers use a range of payment methods. However, criminals have an obvious interest in reducing or eliminating the likelihood that their transactions will be traced. For this reason, the use of payment methods such as wire transfers and gift cards are common, and should be considered a red flag for fraud.



Source | 2017 BBB Scam Tracker Annual Report

# **Top 10 Scams Campaign**

Better Business Bureau's Annual Scam Awareness Campaign

Better Business Bureau's (BBB) National Top 10 Scams list is comprised of scams reported to BBB's ScamTracker® scam reporting tool over the course of the previous year. This list is updated and released in Spring of the following year.

#### Top 10 Scams of 2017 (released March 2018)

- 1. Online Purchase Scams
- 2. Wire Fraud/Spearphishing
- 3. Online Dating Scams
- 4. Employment Scams
- 5. Cryptocurrency Scams

- 6. Income Tax/CRA Scam
- 7. Miracle Weight-Loss Scams
- 8. Advance Fee Loans
- 9. Shady Contractors
- 10. Fake Invoices/Bills

# **BBB's Anti-Scam Pledge**

#### I PLEDGE:

**NOT** to give out personal or financial information to any unknown person even if they claim to be working for a government department or financial institution.

**NOT** to sign up for a free trial offer until I have read all the terms and conditions.

**NOT** to hire a company without having a written contract.

**NOT** to send money in order to win a sweepstakes or lottery.

**NOT** to allow any unknown door-to-door solicitor into my home.

**NOT** to sign any agreement without first reading it.

**NOT** to send money up-front in order to receive a loan.

**NOT** to wire money back to someone who has overpaid me for a good or service.

**NOT** to send money to/for people I met online and do not know.

**NOT** to send money after receiving a distress call/email from a relative unless I have verified that my relative is really in trouble.

**NOT** to forward money or pay an admin fee to a potential employer.

**NOT** to hire a company without doing my homework first. Check their BBB Business Profile, get references, check licensing, insurance and business information.

**TO** let BBB know about any scams happening in my area by filling out the information on ScamTracker® at **bbb.org/scamtracker**.



# **ADVANCE FEE SCAMS**

#### Loans

Advance fee loan brokers promise a loan no matter how bad your credit history is. But once you pay the fee, the loan never comes. Requiring an advanced fee for a loan is illegal in Canada.

Ads for advance fee loans generally appear in classified sections of local and national newspapers, magazines, tabloids, and online. They claim a guaranteed loan even if a consumer has bad or no credit.

#### Nigerian/West African Letters/Emails

These "fund transfer" frauds reach intended victims by email, fax, or traditional letter mail. The sender who claims to be a government official, or member of a royal family, requests assistance in transferring millions of dollars of excess money out of the country with a promise to share with you for your help. Victims are asked to pay a "processing fee" and share their banking info. In the end, they not only lost their money, but gave con artists access to their private accounts.

# Other types of advance fee scams covered in more detail in this Handbook:

- Puppy/Pet Purchase Scams (Page 23)
- Romance Scams (Page 20)

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

- Any up-front fee you need to pay to get a loan is a cue to walk away. Asking for a fee to secure a personal loan is an illegal activity in Canada.
- There are many fees charged for loans. Legitimate lenders will post those fees prominently and collect them from the money they are lending you, but a scammer will try to collect them before you get any money.
- Fees should never be paid via Green Dot, wire transfers, bitcoin, or pre-paid gift cards.
- Be leery when strangers are eager to place unexpected, large amounts of money at your disposal, in exchange for your bank account number and other personal info.
- If you get a letter or email that asks for your help to transfer funds, do not click on any links or download attachments. Report it to BBB and the Canadian Anti-Fraud Centre, then get rid of it.



# **CHARITY & DONATION SCAMS**

Charity scams use deception to get money from individuals believing they are making donations to legitimate charities. This is particularly common in the wake of a natural disaster or other tragedy.

You receive a solicitation from a charity that claims it is collecting donations to help a cause. It may be a postcard in the mail, an email message, a social media post, or even a person going door-to-door.

Charity fraud varies from outright scams to a misrepresentation of how much money actually goes to the charity's clients. It's also important to understand that only donations to legitimate, registered charities are tax deductible. And crowdfunding sites, like GoFundMe, are rarely deductible.

#### Make a Plan for Handling All Charitable Requests

Make a plan and stick to it. Decide at the beginning of the year which charities you can afford to donate to and send your cheques directly to their head offices. When approached by other charities, say that you have already donated to charities of your choice for the current year.

#### WHO TO CONTACT

#### **Canada Revenue Agency**

800-267-2384 800-665-0354 (TTY) www.canada.ca/en/services/taxes/ charities.html

#### Financial & Consumer Affairs Authority of Saskatchewan

306-787-5045 fcaa@gov.sk.ca www.fcaa.gov.sk.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org

- Many appeals are distributed by well-meaning people like your family and friends, but you can't assume they have vetted the charities they ask you to support.
- Get the charity's exact name. With so many charities in existence, mistaken identity is a common problem.
- Be wary of heart-wrenching appeals. What matters is what the charity is doing to help. Ask for specifics on how the money will be used and/or distributed.
- Don't assume that every soliciting organization is tax exempt as a charity. You can readily check a charity's tax status with Canada Revenue Agency.
- Never give out your personal or financial information to anyone over the phone, at the door, or in an email unless you initiated the contact.



# CREDIT REPAIR & DEBT RELIEF SCAMS

In this con, scammers promise to repair your credit or eliminate your debt...for a fee. They entice you with guarantees, such as a particular credit score increase or debt forgiveness, and charge upfront for their "services." If you pay up, scammers either take the money and disappear, or fail to deliver all they promised.

Scammers offering credit repair and debt relief services reach you in a variety of ways: online advertising, social media, or even calling directly (Note: Calling you directly is Direct Selling, and they must have a license from the Saskatchewan Government - which you can freely check - to sell you a product over the phone).

These companies frequently promise - and charge for - impossible services. This includes removing past credit mistakes, such as late payments or a bankruptcy, from your credit report. They may offer to give you a new "credit identity" (the ultimate red flag—this is usually done with a stolen SIN) or negotiate with the lender or credit card company to completely eliminate the debt.

If you are provided with a contract, make sure to read all the details and fine print. Some scammers will put conditions in that you pay for unexpected fees or high interest rates.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

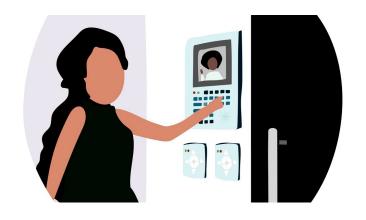
#### Financial & Consumer Affairs Authority of Saskatchewan

306-787-5645 fcaa@gov.sk.ca www.fcaa.gov.sk.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

- Don't believe all claims. Debt can only be forgiven under very specific circumstances, which are not fast or easy. Scammers will take your money and disappear.
- Advance fees are a concern. If a company requests you pay in advance of any actual results, this should be a red flag. In Canada, credit repair and debt relief companies can only collect their fee after they perform the services promised.
- Do not believe guarantees. Nobody can guarantee to make debt go away or improve your credit score. In fact, they can't promise anything before they have even reviewed your personal financial situation.
- Beware the big promise. Follow your instincts - if it sounds too good to be true, it is likely a scam.



# **DOOR-KNOCKER SCAMS**

When the weather is pleasant, direct seller scammers may be knocking on your door. They offer paving services, magazine subscriptions, beauty products, security alarms, and more.

Many door-to-door salespeople are legitimate, but others are looking only to make a sale and move on as quickly as possible.

#### Roaming 'Contractors'

Fake contractors claim they just finished a job nearby and have leftover materials (allowing them to offer a cut-rate price). You pay them cash upfront and they do a terrible job and run. When you check, you can't find their business anywhere.

#### **Alarm System Scams**

Con artists who see security company signs at your home may knock on your door claiming to work for the security company and explain that they're updating systems in your neighbourhood. If you must, read all paperwork, and check with the company immediately about the salesperson's name and the legitimacy of the visit. Better yet, send the person away and make an appointment.

**Utility/Crown Corporation Imposters** 

Scammers impersonate SaskTel, SaskPower, or SaskEnergy representatives to take money or personal info. They frequently threaten residents with deactivation of service unless they pay immediately. Or they enter your home with the intent of stealing valuables.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### **Local Police/RCMP**

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org

#### Financial & Consumer Affairs Authority of Saskatchewan

306-787-5645 fcaa@gov.sk.ca www.fcaa.gov.sk.ca

- Door-to-door (i.e. Direct Sellers)
   <u>must</u> be licensed to operate in
   Saskatchewan by Financial and
   Consumer Affairs Authority
   (a branch of the Saskatchewan
   Government).
- Always receive a copy of any contract. Read everything carefully before signing. Do not feel pressured to sign on the spot.
- Under the *Direct Sellers Act* in Saskatchewan, you have the right to cancel any contract executed at home <u>in writing</u> within 10 calendar days of its execution.
- If you are home alone, pretend that another individual is home with you ("My wife is in the shower.").
- Watch for pushy behaviour. If you are pressured to buy, sign, or let them into your house, shut your door!
- No legitimate utility representative would threaten you.



# **EMPLOYMENT SCAMS**

It may look as though you are starting a great new career, but you are really giving personal information or money to scammers for "training" or "equipment." In another variation, the victim may be "overpaid" with a fake cheque and asked to wire back the difference (See Fake Cheque/ Overpayment Scams, page 15).

Always be wary of work-from-home or secret shopper positions, or any job with a generic title such as caregiver, administrative assistant, or customer service rep. Positions that don't require special training or licensing appeal to a wide range of applicants. Scammers know this and use these otherwise legitimate titles in their fake ads.

Watch out for on-the-spot job offers. You may be an excellent candidate for the job, but beware of offers made without an interview. A real company will want to talk to a candidate before hiring.

And remember to get all details and contracts in writing providing exact details of your work, compensation, vacation, etc.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

#### Government of Saskatchewan Ministry of Labour Relations & Workplace Safety

800-667-1783 www.saskatchewan.ca

- If you didn't apply, you didn't get hired. Be wary of applying for job postings that have too many grammar/spelling errors, lack of job details, and an over-the-top pay scale.
- A reputable employer will give you the equipment you need; they won't give you a cheque to deposit and subsequently wire elsewhere in order to purchase your needed supplies.
- Verify the company's contact information. If they aren't willing to provide a phone number and address you can verify and/or visit, it may be a scam.
- If the job posting is for a well-known brand, check the real company's job page to see if the position is posted there.
- Get all details and contracts in writing providing exact details of your work, compensation, vacation, and others.
- It is illegal in Saskatchewan to charge a fee to the potential employee for employment services.



# FAKE CHEQUE / OVERPAYMENT SCAMS

Fake cheque and money order scams take many different forms, but the underlying con is the same. Scammers take advantage of the fact that many people don't understand the rules about cheque deposits and wire transfers. It is sometimes called the "overpayment scam" because it involves a large initial payment to the target - much more than they are owed for the transaction - and a large refund back to the scammer.

The stories that con artists use vary widely. You might be selling something online and the scammer pretends to be interested in a purchase. Or scammers will "hire" you for a job, such as secret shopping, or tell you you've won a sweepstakes prize. In all cases, the amount of the cheque is "accidentally" far more than the amount agreed to. The scammer instructs you to deposit the cheque, keep the amount owed, and wire back the difference.

When you deposit the cheque, the funds will appear to be available within days. However, forgeries can take weeks to be discovered. Eventually the cheque bounces, but in the meantime you've wired back the "overpayment" to the scammer. A wire transfer is like sending cash; once it's gone, it is very hard to trace.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### **Your Banking Institution**

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

- Be immediately suspicious of overpayments. A cheque can bounce even after your bank allows you to withdraw cash from the deposit.
- Never send money to people you don't know, especially if they ask for the money in an unusual form such as wire transfer or prepaid debit/credit card. Do not share personally identifiable information such as date-of-birth, bank or credit card accounts, passwords, etc. with anyone you do not know. Don't prepay taxes, insurance, or fees on something you have supposedly won.
- Never conduct financial transactions on behalf of strangers.



# HOME IMPROVEMENT/ CONTRACTOR SCAMS

Use caution when hiring a home improvement contractor. Scams abound, especially following a major storm, flood, or other weather event when many homeowners are trying to repair their houses. But contractor scams can happen any time, so be wary of high-pressure sales tactics, upfront fees, and fly-by-night businesses.

Home improvement scams can start with a knock on the door, a flyer, or an ad in the newspaper or online. The contractor may offer a low price or a really short completion timeframe. One common hook is when the scammer claims to be working in your neighbourhood on another project and has leftover supplies.

Once started, a rogue contractor may "find" issues that significantly raise the price. If you object, they threaten to walk away and leave a half-finished project. Or they may accept your upfront deposit and do a terrible job. Or, they claim to need a few extra materials; they take your cheque/cash and never return to do the job.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

#### Local Police/RCMP

#### Financial & Consumer Affairs Authority of Saskatchewan

306-787-5645 fcaa@gov.sk.ca www.fcaa.gov.sk.ca

- Say 'no' to cash-only deals, highpressure sales tactics, high upfront payments, handshake deals without a contract, and on-site inspections.
- Ask for references and check them out. Visit bbb.org to search the business.
- Always get a written contract with the price, materials and job timeline. The more detail, the better.
- Know the law. Work with local businesses that have proper identification, WCB coverage, liability insurance, and municipal/ provincial licensing. Confirm who is responsible for getting permits and who is responsible for cleanup.
- Get up to three quotes before hiring a single company. This way, you know if a price being offered is unusually low or high for the work being done.



# **INVESTMENT SCAMS**

New types of investment scams appear every day. However, most are a variation on one of these common scams.

#### **Offshore Investment**

This scam promises high return from an investment in an offshore market - tax free, of course. But this promise of high returns comes with high risk, and if the promised tax savings are a scam you will likely owe the government money in back-taxes, interest and penalties.

#### **Pension Scam**

If someone tells you there is a way to take the money out of your locked-in retirement account without paying tax, it's likely a scam. In most cases, you can't take any money out until you reach a certain age and there is a limit to how much you can withdraw (plus taxes on that amount).

### **Ponzi/Pyramid Schemes**

Ponzi schemes pay returns to investors from other investors rather than from a profit earned. They usually offer short-term returns that are quite high that other investments cannot guarantee. In Pyramid Schemes, money is exchanged mainly for enrolling other people into the scheme (often no product/service is exchanged). No new money is created, so only the earliest investors benefit.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### Financial & Consumer Affairs Authority of Saskatchewan

306-787-5645 www.fcaa.gov.sk.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

#### **TIPS**

- Know who you are dealing with.
   Anyone who tries to sell you an investment or give you investment advice must be registered unless they have an exemption. Qualified investors will always ask you about your financial situation, objectives, and risk tolerance to find investments that are suitable for you.
- Be cautious at investment seminars/gatherings. The investments themselves may not be scams, but the presenter is often paid to promote specific investments that offer high returns (at high risk).
- Never invest in anything that you don't fully understand. Take your time making investment decisions and never sign documents you have not read carefully.
- Find or search investors/investing companies on bbb.org.

Source: Canadian Securities Administrators



# MEDICAL CURES FRAUD & FALSE BENEFIT CLAIMS

Promotions for medical cures can be found on the Internet, in newspapers, in magazine ads, and in TV infomercials. Generally, these cures are passed on to friends and acquaintances by word of mouth.

#### **Miracle Weight-Loss Scams**

Losing weight is a goal for many Canadians. Be careful, though, as many fat-burning products may only lighten your wallet. Weight-loss scams promise dramatic weight-loss with little or no effort. This may involve the use of unusual diets, "fat-busting" devices, or breakthrough products like pills or patches.

#### **Miracle Cures**

This scam can offer a range of products and services that look like legitimate alternative medicines with quick results. However, health claims need to be rigorously tested in a scientific environment, like human clinical trials, before any direct benefits can be advertised.

#### **Fake Online Pharmacies**

This type of scam uses the Internet and spam emails to offer drugs and medicines at cheap prices and/or without the need of a prescription from a doctor (legitimate online pharmacies will always require one). If you do order and actually receive a product, there is no guarantee it is the real thing.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### Financial & Consumer Affairs Authority of Saskatchewan

306-787-5645 www.fcaa.gov.sk.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker www.bbb.org/council/ad-truth

- Don't trust unsubstantiated claims. Advertised claims regarding a health product's effect must be the result of multiple tests in labs. Consult your healthcare professional.
- Beware of medical cures that are touted to be good for many unrelated diseases.
- Only accept medical advice on the Internet from reliable sources such as the Public Health Agency of Canada (www.phac-aspc.gc.ca) or the Mayo Clinic (www.mayoclinic.com).
- Always check with your doctor or other medical professional before making changes to your medications.
- Ask yourself, if this is really a miracle cure, wouldn't my healthcare professional have told me about it?
- Report any suspicious ads to the Canadian Competition Bureau, and Ad Truth (BBB online tool).



### **ONLINE PURCHASE SCAMS**

Online purchase scams are considered the riskiest form of consumer fraud, according to a new report from the Better Business Bureau (BBB). In 2017, consumers across North America reported more than 47,000 scams to BBB's ScamTracker® program (and that is only 5% of all suspected online purchase scams in the year).

These cons involve purchases and sales, often on eBay, Craigslist, Kijiji or other direct seller-to-buyer sites. Scammers may pretend to purchase an item only to send a bogus cheque and ask for a refund of the "accidental" overpayment (See Fake Cheque/Overpayment Scams, page 15). In other cases, the scammer will simply never deliver the goods or the item you receive was not what was seen/described online.

Check website links and senders' email addresses. A scammer may successfully spoof the look of a legitimate company email, but the email address is usually a dead giveaway that something is not right.

Another common online purchase scam is for counterfeit products. Counterfeit goods mimic original merchandise, right down to the trademarked logo, but are typically of inferior quality. This can result in a life-threatening health or safety hazard when the counterfeit item is medication or an auto part.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### Financial & Consumer Affairs Authority of Saskatchewan

306-787-5645 www.fcaa.gov.sk.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

- An unreasonably low price should be a warning sign. Proceed with caution, even if there's a realisticsounding reason for the price point.
- Pay for purchases through secure payment methods, like a credit card. If a seller asks you to wire money or pay with gift cards, you should decline.
- Scammers copy links, images, and text from legitimate companies. When in doubt, go to the site of the legitimate company separately (do *not* use any links provided in a suspicious email), log into your account, and make sure the purchase information is accurate.



# ONLINE ROMANCE SCAMS

The love bug can hit us at all ages, and in this digital age many relationships are started online. Unfortunately, this also makes it harder to know if a profile is really the truth or not.

Most romance scams start with fake profiles on online dating sites created by stealing photos and text from real accounts or elsewhere. Scammers often claim to be in the military or working overseas to explain why they can't meet you in person. Over a short period of time, the scammer builds a fake relationship with you, exchanging photos and romantic messages, even talking on the phone or through a webcam.

Just when the relationship seems to be getting serious, your new sweetheart has a health issue or family emergency, or wants to plan a visit. No matter the story, the request is the same: they need money. But after you send money, there's another request, and then another. Or the scammer stops communicating altogether.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

- Catfishers (or catphishers) will try very quickly to get you to move to communicating through email, messenger, or phone.
- Be wary of someone who always has an excuse to postpone meeting because they say they are travelling, living overseas or are in the military.
- Do your research. Many scammers steal photos from the web to use in their profiles. You can do a reverse image lookup using a website like images.google.com to see if the photos on a profile are stolen from somewhere else.



#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

# PHISHING SCAMS

Phishing scams can come in the form of prize offers, threatened punishments (like your Netflix or bank account being locked out), and sometimes they just rely on a victim's curiosity to prompt a click or download of something dangerous.

Phishing messages typically use one of three methods to fool victims: 1) the message promises a reward (a gift card, free item); 2) threatens a punishment (unpaid taxes, missed jury duty, deactivated bank account); or, 3) appears entirely mundane (a strangely brief message from an email contact with an attachment or website link).

Phishing scams tend to follow a pattern. You receive an email, phone call or even a text message (called "smishing" or SMS phishing). In the communication, the scammer urges you to click a link, share information, or download an attachment which likely contains malware. In the case of an email or text, the link frequently leads to a form, which prompts the target to enter personal information.

For more tips on Cyber Security, flip to page 33.

- If something sounds suspicious, confirm it by calling the company directly or checking the company website. Don't click on links in an unexpected email - type the URL for the company into your browser or do a web search to find the right website.
- Don't click, download, or open anything that comes from an anonymous sender. This is likely an attempt to gain access to your personal information or install malware on your computer.
- Be cautious of generic emails.
   Scammers try to cast a wide net by including little or no specific information in their fake emails.
   Always be wary of unsolicited messages that don't contain your name, last digits of your account number or other personalizing information.



# PHONE CALL SCAMS

Scammers are tricky, and use every communications option they have to contact you, including the phone.

#### 1-900 Fraud Calls

Consumers receive a mail notice implying they have won a large prize (cash, cars, trips, etc.), and should call a 1-900 number to confirm the amount. What most people don't know is 1-900 and 1-976 numbers are pay-per-call services. You call, are kept on the line for seven to eight minutes, only to find out your winnings were minimal (usually a couple of dollars) but you receive a phone bill for \$35 - \$40.

#### **Dead Air Calls**

You answer a call, but no one is there. This may mean you are receiving calls from an auto-dialer that logs the time the phone is answered. Telemarketers use this info and will try calling again later at the same time.

#### Family/Friend/Grandparent Emergency

This particular fraud has been successfully used in Saskatchewan. Con artists contact potential victims (usually from purchased contact lists or compromised email) and pose as a family member or friend in urgent need of cash. Often the scenario involves an accident or arrest while abroad. They ask for money to be sent to them right away using a transfer service like Western Union or Money Gram.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

#### **National Do Not Call List**

866-580-3625 888-362-5889 (TTY) www.LNNTE-DNCL.gc.ca

- Read through any prize offers you receive and note the odds of winning.
- Some telephone companies offer free services that will block access to all 900/976 numbers; others charge a fee. Check with your telephone provider.
- If you don't recognize the name or number of a caller, let it go to an answering machine. If it's important, you will call them back.
- If you answer the phone and it appears to be a dead air call, hang up!
- If a caller says they are in trouble, determine who the caller is allegedly portraying, hang up, then call the person or their family to verify if the portrayed person is actually travelling or in trouble.
- Register your phone on the National Do Not Call List. This can help limit telemarketers. You will have to renew your registration every five years.



# **PUPPY / PET SCAMS**

If you are looking for a pet to add to your family, be on the lookout for scams. As more consumers turn to the internet to find new pets, more scams are popping up online. According to a 2018 investigative study by Better Business Bureau, experts say a shocking 80% of sponsored advertisements about pets may be fake.

Most puppy scam victims are hooked into the scam by photos of cuddly terriers, miniature bulldogs, or other puppies; other consumers believed they were paying for kittens, parrots, or other animals to be delivered to their homes. While some scammers offer "free" pets, others offer animals for sale at deeply discounted prices. Those paying for the pet are almost always asked to send money through money wiring services like Western Union.

In the typical scam, thieves instruct potential buyers to make up-front payments for shipping, special crates, insurance and other fees associated with transporting the animals.

At times, the thieves may claim the pet is stuck at an airport in transit and additional money is needed for food and water. The requests for money on one pretext or another will continue as long as the victim continues to send money.

In the end, buyers never receive the pets, and lose hundreds to thousands of dollars in the process.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### Financial & Consumer Affairs Authority of Saskatchewan

306-787-5645 www.fcaa.gov.sk.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

- Try to avoid buying your new pet from far away. When you have a pet shipped from another area, you don't know really how healthy or young it is, or even if the pet exists at all.
- Research the breeder and obtain references. Contact those people who have bought puppies from them in the past.
- Being asked for payment in wire transfer, gift cards, or pre-paid cards is a red flag.
- Don't be swayed by a fancy website. Pictures used by scammers are often stolen from legitimate breeders' websites.
- Make sure the price makes sense.
   Do your research and shop around to understand the true value of the animal. A price that seems too good to be true is likely a scam.



# SWEEPSTAKES, LOTTERY & PRIZE SCAMS

You've won a new car or a dream vacation or cash - in a contest you never entered!? This con fools you into thinking you've won a prize or lottery jackpot, but you need to pay upfront fees to receive it. No matter how much you shell out, the winnings never materialize.

You may receive an email or phone call allegedly from a contest organizer, lawyer, judge, customs agent, or other official informing you that you've won a prize. To claim your winnings, you need to first pay taxes, shipping costs, or other fees. You are urged to send the money by wire transfer, or buy a prepaid debit/credit card and share the number and pin with the "contest organizer/ official."

In another version, you receive a letter informing you you've won a jackpot, often from a foreign lottery (Note: It is illegal in Canada and the United States to enter a foreign lottery by phone or mail). The letter includes a seal or other insignia to make it look authentic. There might even be a cheque to cover the taxes on the winnings. You are instructed to deposit the cheque into your bank account and wire or use a prepaid credit card to send the "taxes" to a third party. The cheque is likely fake and the bank will soon inform you - and you will be out the money.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### Financial & Consumer Affairs Authority of Saskatchewan

306-787-5645 www.fcaa.gov.sk.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

- You have to play to win. A
  notification that you have won a
  prize in a contest you do not
  remember entering should be a
  red flag.
- Don't pay upfront fees to claim a prize or check to see if you are a winner, no matter how minor. No legitimate sweepstakes company will ever ask you to pay a fee or buy something that includes paying "taxes," "shipping and handling charges," or "processing fees" to get your prize.
- Be suspicious of irregular communication. Real sweepstakes will not notify you via text or bulk mail. You will not receive unexpected cheques, or be forced to respond in a small timeframe (i.e., 24 hours).
- If you receive a cheque, wait for the bank to clear it before sending/withdrawing money.



# **TECH SUPPORT SCAMS**

A tech support rep calls you at home and offers to fix a computer bug that you haven't even noticed, or a pop-up warning appears on your screen instructing you to dial a number for help.

In this con, scammers pose as tech support employees of well-known computer companies (think Microsoft, Comcast, Norton and Dell) and hassle victims into paying for their "support."

Often the scammer will create a sense of urgency - the computer is sending error messages, they've detected a virus, or your computer is about to crash and you'll lose all your data!

You are told only a tech support employee can fix the problem, and you're asked to allow access to your machine. Once access is granted, the caller will often run a "scan" and claim your computer is infected with viruses. The scammer then offers to fix the problem...for a fee.

That may not be the end of the scam. If you allow remote access, malware may be installed on your machine. Malware often scans files in search of personal information, which scammers can use to commit identity theft.

For more tips on Cyber Security, flip to page 33.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

- Never give control of your computer to a third party unless you know they are a representative of a legitimate computer support team you contacted.
- Legitimate tech support companies do not call out of the blue.
- Look for warning screens. Nearly half of tech support scams begin with an alert on the victim's computer screen. This pop-up will have a phone number to call for help. Instead of calling, shut down your computer and restart it, then run a virus and malware check.
- If you are the victim of a tech support scam, take your computer to a trusted local business and have it checked out, and change the passwords you use to access important online accounts, including online banking.



# **TRAVEL & VACATION SCAMS**

Timeshares and vacation rentals are a great way to travel and have the comforts of home. However, scammers love to take advantage of vacationers by making false promises and creating a sense of urgency to fool them into paying for something that doesn't exist.

In travel and vacation scams, con artists post listings for properties that either aren't for rent, don't exist, or are significantly different than pictured. They then lure vacationers with the promise of low fees and great amenities. Typically, the "owner" creates a false sense of urgency - maybe another vacationer is interested in the rental - to get you to pay up before doing sufficient research.

Another common scam is when a consumer who filled out a ballot at home, boat, or auto shows "wins" a vacation. You will receive a phone call with an offer for a "free" or "low cost" vacation, after you give up your credit card and personal information. You may even be forced to enter into a timeshare agreement that you really don't want.

#### WHO TO CONTACT

#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### Financial & Consumer Affairs Authority of Saskatchewan

306-787-5645 www.fcaa.gov.sk.ca

#### **Better Business Bureau**

888-352-7601 info@sask.bbb.org www.bbb.org/scamtracker

- Talk with the owner. If you are using a service that verifies properties and owners, do not negotiate a rental solely by email. Ask detailed questions about the area. A local owner will have the answers. An owner with vague answers to your question is a red flag.
- Use Google or another search engine to check the address and appearance of the property. Does it match the advertised picture?
- Don't wire or use a prepaid debit/ credit card. Once this money is gone, it cannot be recovered.
- If it sounds too good to be true, it probably is. Do your research to verify.
- Never share your personal or financial information over the phone, by email, or by mail unless you initiated the contact.

# PERSONAL INFORMATION & IDENTITY THEFT



What You Can Do to Protect Your Privacy and Keep Your Identity Safe

Identity theft occurs when a person has used your name and personal information to open an account or order an additional credit card to commit fraud.

#### Signs Your Identity Is Being Used

The following could indicate that your identity is being used fraudulently:

- A creditor informs you that an application for credit (for which you did not apply) was received with your name and address;
- Telephone calls or letters state that you have been approved or denied credit by a creditor to whom you never applied;
- You receive credit card statements or other bills in your name for services that you did not apply for;
- You no longer receive credit card statements or you notice that not all of your mail is delivered;
- A collection agency informs you they are collecting for a defaulted account established with your identity—an account you never opened.

#### **How Con Artists Get Information on Potential Victims**

The skilled con artist has the ability to collate and combine information from several sources to plan an approach to specific potential victims.

Some of these sources are:

- **ATM Skimmers.** Devices are attached to the real ATM card readers that capture your PIN and account numbers.
- Cameras. Cameras are installed to watch as you enter your PIN to access your account.
- **Credit Card Theft.** A thief steals the victim's credit card, credit card statements, or credit renewal card.



What You Can Do to Protect Your Privacy and Keep Your Identity Safe

#### **How Con Artists Get Information on Potential Victims**

- **Free Draw Ballots at Shows.** After the winner is drawn, the remaining cards (with personal information) may be sold to a marketing company.
- **Government Statistics.** Ethnic composition, percentage of seniors, or single residents, as well as other information, can be found by the diligent researcher. Con artists can even target a neighbourhood based on property values.
- **Illegal Sources.** Some criminals can seduce, bribe, or intimidate workers who have access to privileged or personal records and data banks to search and provide information on potential victims.
- **Internet Searches.** A skilled researcher can gain a wealth of comprehensive information from a powerful search engine alone. In some respects, the Internet can provide so much information that the con artists' problem may be to filter out the information that is not needed, rather than to find useful items for the fraud or scam.
- **Mailbox and Dumpster Diving.** A thief goes through the victim's mailbox, trash or the trash of a business looking for personal information found on items such as old bills or credit card application forms that have been thrown in the dumpster without being shredded.
- **Marketing Companies.** These companies legitimately collect and sell information about consumers, including retirement status, address, income, and phone number.
- **Obituaries.** Obituaries not only give the names of people who are bereaved but also list relationships, marital status, the mother's maiden name and even
  - backgrounds, areas of interest, and associations, all of which may be exploited by a con artist. Use initials rather than full first names, and consider shortening what you provide in an obituary (eliminate backgrounds, areas of interest & associations).
- **Phishing.** Con artists may attempt to get personal information by sending an email with a link to a page that resembles a banking page but is actually a page where they can collect your personal information.



What You Can Do to Protect Your Privacy and Keep Your Identity Safe

#### **How Con Artists Get Information on Potential Victims**

- **Questionnaires or Product Registration Cards.** These questionnaires or cards gives others access to some personal information.
- **Shoulder Surfing.** A thief uses observation, such as looking over the victim's shoulder when:
  - The victim is entering his/her personal identification number (PIN);
  - Entering computer passwords in a public location;
  - Filling out a form that asks for personal information.
- **Telephone Numbers and Other Directories.** Many directories include addresses and postal codes, some have reverse directories to help trace numbers, and some business directories contain information on types of occupancy.
- **Tricking You.** Con artists can pretend to be a close or long-lost relative and effectively pry personal information out of you.

#### **How to Minimise Your Risk of Identity Theft**

- Not revealing any personal identifying information before finding out how it will be used and if it will be shared.
- Paying attention to your billing cycles and following up with creditors if your bills do not arrive on time.
- Depositing outgoing mail in post office collection boxes or at your local post office.
- · Promptly removing mail from your mailbox after delivery.
- Forwarding or re-routing your mail if you move or change your mailing address.
- Using passwords on your credit card, bank, and phone accounts. Do not use easily available information such as:
  - Your mother's maiden name
  - Your birth date
  - The last four digits of your SIN (social insurance number)
  - The last four digits of your phone number
- Minimizing the identification information and number of cards you carry.
- Not giving out personal information over the phone, through the mail, or over the Internet unless you have initiated the contact or know with whom you are dealing.

What You Can Do to Protect Your Privacy and Keep Your Identity Safe

#### **How to Minimise Your Risk of Identity Theft**

- Keeping items with personal information in a safe place. Shred or tear receipts, copies of credit applications, insurance forms, physician statements, and credit offers you get in the mail that you do not require.
- Only giving out your SIN when it is required to report income (such as to an employer). Ask to use other forms of identification when possible.
- Not carry your SIN card, passport, or birth certificate with you unless necessary; leave them in a secure place.

#### What to Do If You Suspect Someone Has Stolen Your Identity/SIN/Other Documents

If you suspect someone is using your SIN:

- File a complaint with the police/local RCMP detachment. Ask for the case number and the officer's name and telephone number. Obtain a copy of the police report, make sure it states your SIN and name.
- Contact the RCMP Anti-Fraud Centre at 1-888-495-8501. They can provide advice and assistance about identity theft.
- Call Canada's credit bureaus: TransUnion Canada (1-800-663-9980) and Equifax Canada (1-800-465-7166). Ask for a copy of your credit report. Review it for suspicious activity. If necessary, check to see if your credit file needs to be flagged/frozen on a fraud alert (fees may apply).
- Inform your bank, recipients of stolen cheques, and credit grantors of any theft.
- Report any irregularities in mail delivery to Canada Post. For example, opened letters or missing financial statements.
- Visit a Service Canada office and bring all the necessary documents with you proving fraud or misuse of your SIN. Also bring an original piece of identification, such as your birth certificate.

#### If your Driver's License was stolen:

• Contact SGI immediately to report the theft. They will guide you through the process of re-issuing you a new ID card.

What You Can Do to Protect Your Privacy and Keep Your Identity Safe

#### What to Do If You Suspect Someone Has Stolen Your Identity/SIN/Other Documents

*If your bank cards were stolen:* 

- Notify your banking institution immediately. Notify any credit card companies, such as Visa or MasterCard, of the theft of any of their cards.
- Obtain new accounts, ATM cards, credit cards, cheques, and passwords (do not reuse old passwords) for banking services. Note: Financial institutions are often joint victims and may also suffer financial losses.

When contacting people regarding identity theft:

- Include the police incident or report number in your detailed records;
- Keep detailed records of all conversations and correspondence including names, dates, and what was said.

#### What You Can Do About Identity Theft

- Protect your bank and credit cards by shielding the keypad when entering your PIN
  (personal identification number), checking your statements for questionable
  charges, keeping your cards separate from your wallet, and reporting missing cards
  as soon as you discover they are gone.
- Never use email to send personal information such as your bank account numbers, credit card number, or SIN (social insurance number). Use fax, postal mail, or phone but only if you initiate the call.
- Always to go the bank to change your personal banking information.
- Don't use a public access computer or Wi-Fi when making online purchases or checking your bank balance online in case a thief has installed a keystroke logger or spyware to capture usernames and passwords of website accounts.
- Record and safely store your identification by photocopying them and keeping them stored in a safety deposit box or other safe location.

#### WHO TO CONTACT

**Your Local Police or RCMP** 

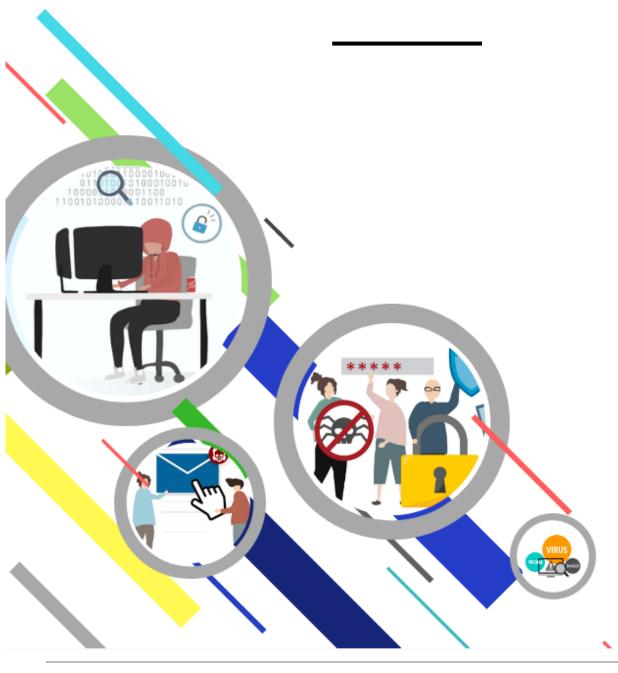
#### **Canadian Anti-Fraud Centre**

888-495-8501 www.antifraudcentre.ca

#### Service Canada

800-206-7218 (select option "3") 800-926-9105 (TTY) www.canada.ca

# CYBER & EMAIL SECURITY



# Let's Talk Cyber Security

Keep Your Computer—and Your Personal Information—Safe from Cyber Criminals

Whether you are banking online, connecting with friends, sending emails, or checking out the real estate market in your area, the Internet has become an essential part of everyday life.

What you may not know is that this amazing resource is also a breeding ground for criminal activity—where your every move can be monitored and your information compromised.

But if you take the time to learn about common threats and risks, online security and protecting yourself can be easy.

#### What Is the Difference Between Viruses, Trojans, Worms and Other Malware?

**Malware is short for malicious software.** This is a general term used to describe all the viruses, worms, spyware and anything else designed to harm your computer and steal your personal information.

**Viruses wreak havoc on your files.** A virus is a program that copies itself and infects multiple files on your computer. As those files are copied and shared, the virus can begin to affect other computers as well.

#### Spyware steals your information.

Spyware collects your personal information and sends it back to the spyware's creator. This could include your passwords, page browsing and video watching habits, changing your homepages or other computer functions, 110010 installing obnoxious tools, or stealing your account and credit card credentials.

**Trojan Horse creates a back door.** These are applications that look like they are doing something innocent, but secretly have malicious code that allow hackers to remotely control or view your computer without you knowing.

Worms infect through the network. Computer worms use networks to duplicate themselves and affect multiple computers quickly. They usually gain access through a security hole, like an email attachment that is easily opened.



### Let's Talk Cyber Security

Keep Your Computer—and Your Personal Information—Safe from Cyber Criminals

#### What You Can Do to Keep Your Computer Cyber Secure

- Install anti-virus, anti-malware, and anti-spyware software to keep your computer and network protected. It is important to keep your protection up-to-date by purchasing new software or updates annually.
- Keep your computer's operating system software up-to-date by downloading and installing any updates or patches as soon as they are available.
- Change any default password settings for your computer, Wi-Fi, and other connected devices to be more secure.
- If a device does not need to be connected to the Internet at all times, consider turning its connection off—or just turning the device off entirely. If it isn't connected, it can't download a virus or be accessed by a cyber criminal.
- Turn off your computer's microphone and camera when not in use. These can be hacked and used against you.
- Listen to your instinct. If something seems strange, disconnect and run a virus/malware/spyware scan right away. Find local, professional technical help if needed.

#### **How to Create a Strong Password**

- A minimum of eight characters.
- Use a combination of uppercase and lowercase letters, and numbers.
- Include at least one character that is special (i.e.,  $!\#\sim/^*$ -).
- Be creative. Use the first letter of each word from a memorable sentence or phrase, then make it even harder by changing letters into numbers, like using 3 instead of E.



#### WHO TO CONTACT

Canadian Anti-Fraud Centre 888-495-8501 www.antifraudcentre.ca

### **Let's Talk Email Security & Tips**

What You Should Look for to Spot Malicious Emails

Email has become an essential part of life, with more and more people using email to stay in touch over using a phone to call. It is a means to have conversations with friends and family all at once, receive shopping and shipping confirmations, verify trip itineraries, and more.

Email is also one of the easiest ways for cyber criminals to target ordinary citizens. A good rule of thumb is if an email looks suspicious for any reason, just delete it. If it is coming from a friend or family member, they will try again or find another way to contact you.

But if you know what to look for, you will be better able to protect your computer and your personal information.

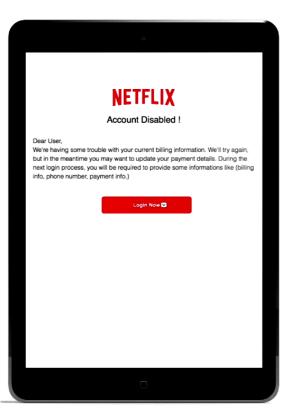
#### **Top 10 Spam Email Subject Lines**

If you receive an email with one of these subject headings, be on the alert! These kinds of email messages are frequently used by fraudsters to get your attention and make you take action (like calling a 1-900 number) or click on links you shouldn't. These attacks are effective in that they try to get the target to

either avoid a negative consequence or gain something of value.

#### Common email attack subjects are:

- Microsoft: Re: Important Email Backup Failed
- Microsoft/Office 365: Re: Clutter Highlight
- [Bank Name]: Your [Bank Name] contact information has been updated
- [Bank Name]: Fraudulent Activity On Your Chequing Account Act Now
- Office 365: Change Your Password Immediately
- Amazon: We tried to deliver your package today
- Amazon: Refund Valid Billing Information Needed
- IT: Ransomware Scan
- Docusign: Your Docusign account is suspended
- You have a secure message



### **Let's Talk Email Security & Tips**

What You Should Look for to Spot Malicious Emails

#### **Tips for Spotting a Bad Email**

1. Look closely at the sender's address. Does it appear to be coming from a legitimate source? Dig a little deeper than just the first and last name or company department that initially appears in the Sender's field, identify what the sender's actual email address is and think, "Does this seem right?"



2. Links inside an email are often wearing a mask. A link to a website may simply display as "Login Here" rather than contain the actual web address. So what should you do? Hover your mouse over that link, but *don't click*, you should be able to see where that link would be taking you *if you clicked it*. Does it seem legitimate?

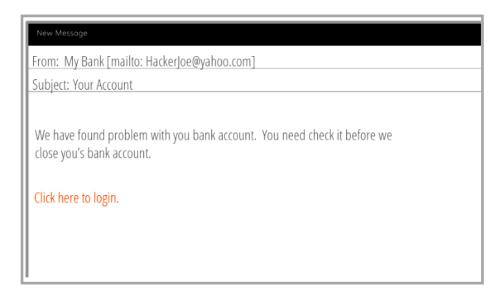


### **Let's Talk Email Security & Tips**

What You Should Look for to Spot Malicious Emails

#### **Tips for Spotting a Bad Email**

3. English is not always the first language of a hacker. Check the verbiage in the body of the email. If the email is supposed to be from your bank, does it seem like something your bank would write?



4. If you have an email that contains attachments, use extreme caution when/if you open that attachment. Think to yourself, "Why is this person sending me this attachment?" Are you getting a Word document from a complete stranger? Sure, you may be curious, but better to forever remain curious than to become a victim by opening that attachment and unknowingly installing malware.



# PERSONAL & HOME SAFETY



### **Your Personal Safety Matters**

Plan for Your Personal and Financial Safety in Case of Abuse or Emergency

Abuse can be a hard word to accept. People from all walks of life have found themselves in abusive relationships - it can happen to anyone. Everyone has the right to be safe and free from abuse.

#### What You Can Do About Abuse

- Tell someone you trust about the abuse. Choose individuals who will respect your decisions and who can listen without telling you what to do. You might want to ask them to just listen so that they don't feel pressure to solve the problem for you.
- You may need to plan some next steps. Those steps should be realistic. You are the expert in your own life and the best person to decide what you can do to set limits and to increase your safety.
- If you are afraid the situation will get worse, make a safety plan that includes where you can go in an emergency and what you will take with you. Think about where you will stay and how you will get there.
- Consult a lawyer or legal service about your rights and options (your local seniors' organization can help you find a lawyer or service).
- Keep track of your financial statements and other legal documents. Talk to your bank about how to protect your assets.
- Visit your local library, health and community centre to find out information about other services that are available to support you.
   If you live with the abusive person and want to look for services on your home computer, be sure to cover your tracks by erasing the history.
- If you are ever in danger, call 9-1-1 or the local police.



### **Your Personal Safety Matters**

Plan for Your Personal and Financial Safety in Case of Abuse or Emergency

#### Take Care of Your Physical and Mental Wellbeing

- Know your rights everyone has the right to be safe and free from harm at home and in the community.
- Stay in regular contact with people who support you and respect your decisions.
- If you are often alone, make the effort to connect with someone you care about and talk about how you can become more involved in your community. There are seniors' organizations in many communities that offer activities and events where you can meet people.
- Reach out to other seniors who may be alone. Thinking of others is a good way to make a contribution to the whole community.
- Involve yourself in meaningful activities that give you enjoyment, strength and comfort. Go on outings with friends, volunteer, attend church, join a gym, or visit your neighbours.
- Stay physically active. Eat regularly and well.
- If you feel depressed and have no one to talk with, seek support from a friend, your minister, priest, faith leader, or from social service agencies in your community. You don't have to be alone with problems. There is no shame in asking for help.

#### **Home Safety**

Most people feel safe in their own home. However, many do not take the required precautions to secure their homes against break-ins and unlawful entry.

- · Conduct security checks to determine where weaknesses or points of entry may exist.
- Ensure entrances are well lit. Consider purchasing an outdoor security camera.
- Install good locks and always use them.
- Never open your door to strangers.
- Change your routine as burglars often monitor their targets prior to a break-in.
- Mark valuables for easy identification.
- Keep your screen door locked. Install a screen door if you don't have one.

### Home Fall Prevention Checklist

Whether it is enjoying the summer out at the lake or working on a hobby at home, we all strive to lead full, independent lives doing the things we enjoy with the people we love. An important part of maintaining that independence is ensuring we have a safe living environment to reduce the risk of injury. Research has shown that slips, trips and falls cause the most incidents around the home. Because of this, the Saskatchewan Safety Council has dedicated itself to researching resources on fall prevention and providing them to you here.





# LIVING ROOM & BEDROOM

### Do your floor rugs and mats have non-skid backing on them?

• Install non-skid backing on them to prevent them from sliding when they are being walked on.

### Do you have emergency lighting in the living room?

• It is extremely difficult to get around when the power goes out, especially at night. Keep a flashlight in an easy to find spot and install rechargeable, motionsensing lights.

### Are there clear walking paths to the exits?

• Furniture should be arranged so it is easy to navigate around the room, especially in the dark.

# Are your traffic areas clear of wires and cables?

- Use a cord protector to cover wires that run through high traffic areas.
- Switch to a cordless telephone to reduce loose wires.
- Move lamps and other devices closer to plug-ins so the cords do not need to stretch or lie across high traffic areas.



# BASEMENT & LAUNDRY

#### Is your laundry room organized?

- Place a non-slip mat in front of your washing machine to prevent slipping on water.
- Have a table where you can set your laundry basket for easy lifting and clothing transfer.
- Ensure that water flows naturally towards the floor drain. Call a professional immediately if you notice pools of water.
- Many laundry rooms are in storage areas or furnace rooms with open piping and wires. Make sure you can navigate the room safely while carrying your laundry items.

### Additional basement fall prevention tips:

- You should always be able to walk to your breaker box, furnace, and other appliances without any obstructions in the way.
- Do not place objects at the bottom of the basement stairs.



### Are your stairways and hallways well lit?

- Install a light switch at the top and bottom of each stairway so you are never using the stairs in the dark.
- Keep a flashlight near the stairs to help you see at night and during emergencies.

### Do your stairs provide proper walking support?

- Install hand rails on both sides of the stairway. Have a professional install them to ensure they are the correct height and properly secured.
- Place non-slip stair treads on wood and laminate stairs.

#### Are your stairs in good condition?

• If your stairs squeak, bend, or feel loose when you walk on them, call a professional to inspect them and make any necessary repairs.

### Are your stairways and hallways free of hazards?

- Never place items at the top or bottom of stairways or on any steps.
- Hallways should always be free of clutter.
- If you have rugs in your hallway, install non-skid backing on them to prevent them from sliding.



#### **BATHROOM**

### Is your bathtub and/or shower equipped for fall prevention?

- Place a non-slip bath mat on the floor of your bathtub/shower. It should run the length of the surface.
- Install a grab bar in a place that helps you get in and out of the bathtub.
   Make sure it is secured into wall studs.
- Use a shower organizer to help organize soaps, shampoos and other bath products. This will avoid bending over to reach them.
- If you have mobility problems, consider using a safety chair in the bathtub. If you do, consult a physician and/or a mobility specialty store in order to help you pick the right chair.

### Does your bathroom have proper lighting?

 Install a rechargeable motion-sensing light to help you see at night or during a power outage.

### Additional bathroom fall prevention tips:

- Place a non-slip mat outside the bathtub and in front of the vanity to contain any spilled water.
- Make sure you are completely dry before leaving the bathroom.
   Tracking water into other rooms greatly increases fall risks.



#### **KITCHEN**

### Are your kitchen items properly stored?

- Place your most used pots, pans, plates, etc. in cupboards and on shelves that are at or near chest level to make them easily accessible.
- Keep your large, heavy items in lower cupboards and lighter items in higher ones. This makes it easier on your back and large items will not fall on you if you lose your grip (Remember: always lift with your legs).

#### Is there enough light in your kitchen?

 Kitchens are full of dangerous objects that can harm you if you fall. Make sure your light is strong enough to illuminate all areas of the floor.

### Are your cupboards and drawers in good working condition?

- Fix any cupboard doors and drawers that do not open and/or close properly.
- If possible, renovate your cabinet doors and drawers with the ability to soft-close. This helps close them the last few inches if you don't push hard enough.



#### **KITCHEN** (continued)

## Additional kitchen fall prevention tips:

- Keep a CSA approved step stool in the kitchen and use it to reach high places. Never use a chair or pull yourself up on to the counter.
- Place a non-slip mat in front of your kitchen sink to trap spilled liquids.
- Use a long-handled mop to clean up spills. This will give you more stability and you will avoid walking in the spill.

- Store heavy objects on lower shelves.
- Install additional lighting that is motion sensing or automatically comes on when the garage door opens.

### Additional outside-the-home fall prevention tips:

- Cut your grass on a regular basis. Tall grass can hide trip hazards.
- Ensure walkways to your front and back door are properly lit. Solar lights are a great solution.
- Use cordless mowers and garden tools to avoid running an extension cord around the yard.



#### **OUTSIDE THE HOME**

# Are walkways clear of objects and in good condition?

- Put all yard tools back into their proper storage when finished with them.
- Keep garden hoses rolled up.
- Remove snow as soon as possible to prevent ice build-up and keep ice melt at each doorway for easy access.
- Have cracks and/or broken portions of walkways repaired.

### Is your garage organized and clutter-free?

• Store tools off the floor and out of the main walk paths.



#### **GENERAL**

#### Know your limits.

- Over-stretching to grab something off a shelf or lifting an object that is too heavy greatly increases your risk of a fall.
- Exercise regularly. It will help keep your muscles strong, which is key to maintaining balance and coordination.
- Have your vision checked at least once a year. Poor vision greatly increases your risk of falling.
- If you aren't feeling well, take extra time to do your tasks throughout the day and rest whenever you need to.



#### **GENERAL** (continued)

#### Understand your health.

- If you have a medical condition that makes you more prone to falls, consider wearing an emergency alarm device.
- Talk with your pharmacist to understand prescription and overthe-counter medication side effects. Take extra precautions with ones that make you sleepy or dizzy.
- If you have mobility problems, talk to your doctor about mobility aids such as canes, wheeled walkers, and stair lifts.
- Miscellaneous.
- If you have to run power cords a long distance or you need to use an extension cord, have an additional electrical outlet installed near the objects instead.
- Keep items away from main entrances to ensure ease of access both in and out. This will also ensure emergency first responders can get to you quickly if needed.
- If you aren't getting enough light, increase the wattage of your light bulb if the fixture supports it or install a new fixture that can.
- Always use a step-ladder to change a light bulb. Ask for assistance if you can't safely reach the fixture.

- Vacuum on a regular basis to keep from stepping on small and/or sharp objects such as pins or broken glass.
- Keep a list of the following emergency numbers near each of your phones:
  - Doctor
  - Immediate family members
  - Fire and Police departments
  - Healthline 8-1-1

If you have an immediate emergency, dial 9-1-1.

If you find a hazard that requires a professional to repair, the Government of Saskatchewan's Financial and Consumer Affairs Authority, Consumer Protection Division has a guide for hiring a contractor. The information in this guide will help you choose someone that will treat you fairly and with respect. You can also use this to help you hire a specialized professional such as a plumber or electrician. Call them at (306) 787-5550 or (877) 880-5550 (toll free).

Better Business Bureau also provides a comprehensive database of service professionals. Transparent complaints, customer reviews, and ratings will help you find a local professional you can trust. Visit **bbb.org/sask** or call **(888) 352-7601**.

# ADDITIONAL RESOURCES & CONTACTS



### Consumer Complaints and Door-to-Door Sales

Canadian Anti-Fraud Centre (RCMP)
(888) 495-8501
antifraudcentre-centreantifraude.ca

Saskatchewan Government Financial & Consumer Affairs Authority (306) 787-5645 fcaa.gov.sk.ca/fcaa411

Better Business Bureau of Saskatchewan (888) 352-7601 (toll free) 980 Albert Street Regina, SK S4R 2P7 www.bbb.org/sask

#### Reporting Lost or Stolen Credit Cards, Identity Theft, or Checking Your Credit Rating

Equifax National Consumer Relations 866-828-5961 P.O.Box 190, Station Jean-Talon Montreal, QB H1S 2Z2 www.equifax.ca

TransUnion Canada Customer Relations Department 800-663-9980 P.O.Box 338, LCD1 Hamilton, ON L8L 7W2 www.transunion.ca

#### **Reporting Problems with Direct Mail**

(may reduce the number of marketing offers received by mail)

Canadian Marketing Association (416) 391-2362 / (800) 267-8805 www.the-cma.org/consumers

# **Checking the Validity of Charitable Organizations**

Canada Revenue Agency Charities Listing (800) 267-2384 / (877) 442-2899 www.cra-arc.gc.ca/chrts-gvng/lstngs/ menu-eng/html

Better Business Bureau Wise Giving Alliance www.give.org

#### Registering Your Home Phone, Cellular Phone, or Fax Numbers with the National 'Do Not Call' List (NDNCL)

(866) 580-3625 toll free (888) 362-5889 for the hearing impaired (TTY device) www.LNNTE-DNCL.gc.ca

Note: You must be calling from the number you wish to register, and you must renew your registration every five years (this can be done by phone or online).

## **Investigating or Reporting Renovation and Repair Fraud**

Saskatchewan Home Builders Association

Note: Grievances must be for a building code concern, and can only be made against <u>current</u> SHBA members.

Regina Branch (306) 546-5226 www.reginahomebuilders.com

Saskatoon Branch (306) 955-5188 www.saskatoonhomebuilders.com

Better Business Bureau of Saskatchewan (877) 352-7601 www.bbb.org/sask (to file a complaint) www.bbb.org/scamtracker (to report a scam or fraud incident)

#### **Reporting Fraud or Scams**

Canadian Anti-Fraud Centre (RCMP)
(888) 495-8501
www.antifraudcentre-centreantifraude.ca

Better Business Bureau of Saskatchewan (888) 352-7601 www.bbb.org/scamtracker

Canada Spam Email Reporting Centre https://ic.gc.ca/eic/site/030.nsf/eng/ h\_00017.html

#### Requesting Info on a Variety of Issues Related to Older Adults Including: Financial Abuse, Mental/Physical Abuse, Scams, Health, Recreation, etc.

Saskatchewan Seniors Mechanism (306) 359-9956 (306) 359-6922 fax 112-2001 Cornwall Street Regina, SK S4P 3X9 info@skseniorsmechanism.ca www.skseniorsmechanism.ca

Saskatchewan Safety Council (306) 757-3197 Regina (306) 343-2023 Saskatoon (855) 280-7115 Toll Free in SK 445 Hoffer Drive Regina, SK S4N 6E2 contact@sasksafety.org

#### Saskatchewan 2-1-1

2-1-1 is a free, confidential information and referral system for thousands of community and social services across Saskatchewan.

Dial or text 2-1-1 anywhere in Saskatchewan https://sk.211.ca

#### **Reporting Advertising Issues**

Canadian Competition Bureau (800) 348-5358 www.competitionbureau.gc.ca

Saskatchewan Government Financial & Consumer Affairs Authority (306) 787-5645 info@fcaa.gov.sk.ca fcaa.gov.sk.ca/fcaa411

Better Business Bureau Ad Truth Reporting Tool www.bbb.org/council/ad-truth

#### **Other Online Resources**

Canadian Centre for Elder Law www.bcli.org/be-savvy

Government of Canada Office of Consumer Affairs
www.ic.gc.ca/eic/site/oca-bc.nsf/eng/
h ca02207.html

Royal Canadian Mounted Police www.rcmp-grc.gc.ca

Saskatchewan Association of Chiefs of Police www.sacp.ca

Snopes (scam info website) www.snopes.com

#### **Other Local Resources to Consider**

Elder Abuse Organizations
Legal-Aid Clinics for Seniors
Community Information Centres
Crime-Prevention Organizations

#### **Crime Stoppers Tip Line**

Moose Jaw Crime Stoppers (800) 222-8477

Prince Albert Crime Stoppers (800) 222-8477 www.pacrimestoppers.ca

Regina Crime Stoppers (800) 222-8477 www.reginacrimestoppers.ca

Saskatchewan Crime Stoppers (800) 222-8477 www.saskcrimestoppers.com

Saskatoon Crime Stoppers (800) 222-8477 www.saskatooncrimestoppers.com

#### **Municipal Police Services in SK**

Caronport Police Service (306) 756-2522

Corman Park R.M. of Corman Park Police Service (306) 242-8808

Dalmeny Police Service (306) 254-2114

Estevan Police Service (306) 634-4767

File Hills First Nations Police Service (306) 334-3222

Luseland Police Service (306) 372-4844

Moose Jaw Police Service (306) 694-7600

#### **Municipal Police Services in SK**

(continued)

Prince Albert Police Service (306) 953-4222

Regina Police Service (306) 777-6500

Saskatoon Police Service (306) 975-8300

Vanscoy Police Service (306) 291-6050

Weyburn Police Service (306) 848-3250

#### Royal Canadian Mounted Police Detachments in SK

Assiniboia Detachment (306) 642-7110

Avonlea Community Detachment (306) 868-2300

Balcarres Community Detachment (306) 334-3210

Battlefords Municipal Detachment (306) 446-1720

Beauval Detachment (306) 288-6400

Bengough Community Detachment (306) 268-2144

Big River Detachment (306) 469-2590

Biggar Detachment (306) 948-6600

Birch Hills Community Detachment (306) 749-2200

### Royal Canadian Mounted Police Detachments in SK

Blaine Lake Detachment (306) 497-3600

Broadview Detachment (306) 696-5200

Buffalo Narrows Detachment (306) 235-6660

Cabri Community Detachment (306) 778-5550

Canora Detachment (306) 563-4700

Carlyle Detachment (306) 453-6707

Carnduff Detachment (306) 482-4400

Carrot River Detachment (306) 768-1200

Colonsay Community Detachment (306) 255-3700

Coronach Detachment (306) 267-1830

Craik Detachment (306) 734-5200

Creighton Detachment (306) 688-8888

Cumberland House Detachment (306) 888-5550

Cut Knife Detachment (306) 398-3500

**Deschambault Community Detachment** 

(CTA)

(306) 632-2392

Delisle Community Detachment (306) 493-3240

Royal Canadian Mounted Police Detachments in SK (continued)

Elbow Community Detachment (306) 854-1830

Esterhazy Detachment (306) 745-4740

Estevan Detachment (306) 637-4400

Eston Community Detachment (306) 962-8530

Fillmore Community Detachment (306) 722-3400

Foam Lake Community Detachment (306) 272-6660

Fond du Lac Detachment (306) 686-2060

Fort Qu'Appelle Detachment (306) 332-2222

Glaslyn Community Detachment (306) 342-2005

Gravelbourg Detachment (306) 648-4350

Green Lake Community Detachment (306) 832-4810

Greenwater Detachment (Rose Valley) (306) 322-2550

Gull Lake Community Detachment (306) 672-3140

Hafford Community Detachment (306) 549-4280

Hanley Community Detachment (306) 544-3400

Hudson Bay Detachment (306) 865-5550

Humboldt Detachment (306) 682-2535

Ile A La Crosse Detachment (306) 833-6300

Indian Head Detachment (306) 695-5200

Ituna Community Detachment (306) 795-6400

Kamsack Detachment (306) 542-5560

Kelvington Detachment (306) 327-1200

Kerrobert Community Detachment (306) 834-6550

Kindersley Detachment (306) 463-4642

Kipling Community Detachment (306) 736-6400

Kyle Detachment (306) 375-5510

La Loche Detachment (306) 822-2010

La Ronge Detachment (306) 425-6730

Langenburg Community Detachment (306) 743-5600

Lanigan Detachment (306) 365-1370

Leader Detachment (306) 628-4600

Lloydminster Municipal Detachment (306) 825-6350

Loon Lake Detachment (306) 837-2440

Royal Canadian Mounted Police Detachments in SK (continued)

Lumsden Detachment (306) 731-4270

Maidstone Community Detachment (306) 893-4800

Maple Creek Detachment (306) 662-5550

Martensville Community Detachment (306) 975-1610

Meadow Lake Detachment (306) 236-2570

Melfort Detachment (306) 752-6420

Melville Detachment (306) 728-1700

Milestone Detachment (306) 436-6250

Montmartre Community Detachment (306) 424-6400

Moose Jaw Detachment (306) 691-4670

Moosomin Detachment (306) 435-3361

Morse Detachment (306) 629-4100

Naicam Community Detachment (306) 874-2142

Nipawin Detachment (306) 862-6270

North Battleford Detachment (306) 446-1720

Onion Lake Detachment (306) 344-5550

Outlook Detachment (306) 867-5440

Pelican Narrows Detachment (306) 632-3300

Pierceland Detachment (306) 839-3330

Pinehouse Detachment (306) 884-2400

Ponteix Detachment (306) 625-6400

Porcupine Plain Community Detachment (306) 278-8180

Prince Albert Detachment (306) 765-5501

Punnichy Detachment (306) 835-5200

Radisson Community Detachment (306) 827-3460

Radville Community Detachment (306) 869-4600

Rose Valley (Greenwater) Detachment (306) 322-2550

Rosetown Detachment (306) 882-5700

Rosthern Detachment (306) 232-6400

Sandy Bay Community Detachment (306) 754-4600

Saskatoon Detachment (306) 975-5173

Saskatchewan Headquarters (F.Div.) (306) 780-5461

Shaunavon Detachment

(306) 297-5550

## Royal Canadian Mounted Police **Detachments in SK** (continued)

Shellbrook Detachment (306) 747-2606

Smeaton Community Detachment (306) 426-2630

Southend Detachment (306) 758-5670

Southey Detachment (306) 726-5230

Spiritwood Detachment (306) 883-4210

St. Walburg Community Detachment (306) 248-6250

Stanley Mission Community Detachment (FNP) (306) 635-2390

Stony Rapids Detachment (306) 439-2185

Strasbourg Community Detachment (306) 725-3520

Sturgis Detachment (306) 548-6250

Swift Current Municipal Detachment (306) 778-4870

Swift Current Rural Detachment (306) 778-5550

Tisdale Detachment (306) 878-3810

Turnor Lake/Birch Narrows Community Detachment (FNP) (306) 894-4420

Turtleford Detachment (306) 845-4520

Unity Detachment (306) 228-6300

Vonda Community Detachment (306) 258-3270

Wadena Detachment (306) 258-3270

Wakaw Detachment (306) 233-5810

Warman Detachment (306) 975-1670

Waskesiu Lake Detachment (306) 663-4400

Watrous Detachment (306) 946-3316

Weyburn Detachment (306) 848-4640

White Butte Detachment (306) 781-5050

Wilkie Community Detachment (306) 843-3480

Wollaston Lake Detachment (306) 633-1200

Wynyard Municipal Detachment (306) 554-5550

Yorkton Municipal Detachment (306) 786-2400

Yorkton Rural Detachment (306) 786-4500