Saint John Police Force
Current Scams Trending in Saint John
&
Fraud Prevention Facts

This information will be updated frequently as new trends emerge relating to frauds and scams that are active in our City.

Included are some top trending scams that are trending right now that you should be aware of when you are surfing the internet. You can query these topics on the internet to see what is out there. The more informed you are, the safer you are on the net.

- CRA Scam
- Romance scam
- Outstanding parking ticket scam
- Phone company payment scam
- Credit Card scam
- Pay Pal scam
- Overpayment scam

Helpful links:

www.antifraudcentre.ca – Canadian Anti Fraud Center

www.nbsc-cvmnb.ca – New Brunswick Securities Commission.

www.competitionbureau.gc.ca – Competition Bureau.

www.scambusters.org – Scambusters originates from the United States but the content is similar to Canadian content and shares information on similar scams.

Top trending scams in Saint John area 2016/2017

1. **Romance Scam**

   They met online. He said he was a friend of a friend. The woman, in her 50s and struggling in her marriage, was happy to find someone to chat with. "He was saying all the right things," she remembered. "He was interested in me. He was interested in getting to know me better. He was very positive, and I felt like there was a real connection there."

   That connection would end up costing the woman $2 million and an untold amount of heartache after the man she fell in love with—whom she never met in person—took her for every cent she had.

   It's called a romance scam, and this devastating Internet crime is on the rise. Victims—predominantly older widowed or divorced women targeted by criminal groups usually from Nigeria—are, for the most part, computer literate and educated. But they are also emotionally vulnerable. And con artists know exactly how to exploit that vulnerability because potential victims freely post details about their lives and personalities on dating and social media sites.

   The Internet makes this type of crime easy because you can pretend to be anybody you want to be. You can be anywhere in the world and victimize people," she said. "The perpetrators will reach out to a lot of people on various networking sites to find somebody who may be a good target. Then they use what the victims have on their profile pages and try to work those relationships and see which ones develop."

Don't Become a Victim

To stay safe online, be careful what you post, because scammers can use that information against you. Always use reputable websites, but assume that con artists are trolling even the most reputable dating and social media sites. If you develop a romantic relationship with someone you meet online, consider the following:

Research the person's photo and profile using online searches to see if the material has been used elsewhere. (right click, copy photo, go to Google images paste in search field)

Search the person's name on line. For example type "John Smith scam" see what names are trending as fraudulent identities.

Never send money or wire money to anyone you don't know personally. "If you don't know them, don't send money.

2. CRA (Canada Revenue Agency) Scam

You may get a phone call from a person aggressively telling you to pay the taxes you owe. This person will claim to be from the Canada Revenue Agency or a Police Agency. They may threaten arrest, jail and other tactics to scare you in to paying promptly. The person speaking to you may sound very convincing and reference names and places you know locally to sound more legitimate. The trend in the Saint John area is that the fraudster tells you that you can pay your "outstanding bill" by purchasing iTunes cards or other gift cards.

Conversely, these scams may insist that your personal information is needed so that the taxpayer can receive a refund or a benefit payment.

Taxpayers should be vigilant when they receive, either by telephone, mail, text message or email, a fraudulent communication that claims to be from the Canada Revenue Agency (CRA) requesting personal information such as a social insurance number, credit card number, bank account number, or passport number. Also, CRA will never threaten you, call the Police to arrest you, or ask you to pay any outstanding bill by iTunes cards or any other gift card to pay outstanding taxes.

Here are some examples of current CRA scams.

Sample telephone scam
http://www.cra-arc.gc.ca/scrty/frdprvntn/frdlnttlphn-eng.html

Samples of Fraudulent Online Refund Forms
http://www.cra-arc.gc.ca/scrty/frdprvntn/nln-rfnd-eng.html

Sample of text message
http://www.cra-arc.gc.ca/scrty/frdprvntn/mbltxtmssgs-eng.html

Sample of fraudulent letter
http://www.cra-arc.gc.ca/scrty/frdprvntn/frdlntlttr-eng.html

3. Parking ticket scam

Scammers are sending out emails to thousands of motorists claiming they've received a bogus parking ticket. Fraudsters are sending out emails entitled " Reminder To Ticket Keeper " that look as if they are from a legitimate company called "impark" and has these logos attached:

impark
your parking authority

Imperial Parking
A Customer Driven Company

The email says you have a parking ticket and encourages the reader to click on a link to 'payment options and photos' to find out more about your fine and how to pay. However, the link is likely to contain malware that would allow criminals to access information on your computer, or monitor the websites you visit and your keystrokes allowing scammers to get hold of your personal information.

4. **Phone bill scam**

You may have received an email from (Telus, Rogers, Bell, Virgin, Fido, etc…) indicating that your monthly payment was recently declined due to insufficient funds or that your credit card was expired etc….. The scammers then provide a link for you to "UPDATE YOUR BILLING INFORMATION" This is a scam and you will be giving scammer's direct access to your credit card information.

5. **Employment or Overpayment Scams**

Scammers use online classified websites like Kijiji, Craigslist, Monster, Indeed, and Workopolis to recruit potential victims. The most common scams include Mystery Shopper, Homecare worker, nanny, and housekeeping. Consumers are offered a job after responding to an online ad or a text message. The victims receive a cheque in the mail with instructions to complete local purchases and send unspent funds through a money service business.. Eventually, the cheque is returned as counterfeit and the "employee" is accountable to pay for the funds that were wired. Another common job scam involves the victim acting as a financial receiver/agent. Victims are told to accept payment in their personal account (often by eTransfer or cheque), keep a portion and forward the remaining amounts to third party "employees" or "companies". Victims are eventually advised by their bank that the original payment was fake or fraudulent and any subsequent monies sent are therefore paid out of the victim's own pocket. Scammers will attempt to process as many payments as possible before the victim's financial institution advises that the original payment was fake.

6. **Microsoft Scam (Hang up on tech experts claiming your computer has a virus. It's a scam!!)**

This scam involves a cold call from the scammer posing as an employee from Microsoft or a computer anti-virus company. The victim is advised that they have outdated anti-virus software, spyware or errors on their system, and they are at risk from hackers. The victim is then unknowingly led to a site that facilitates remote access to your computer. Once the caller has remote access to your computer, any personal information that you have on your system such as passwords, credit card numbers, and account numbers can be obtained. Microsoft will not call you about error reports from your computer. Any reputable software company would not trick you into allowing remote access to your computer. This is what they would be trying to protect you from. If you receive a call like this, hang up the phone.

7. **Credit Card Scams**

The trending credit card scam in Saint John is initiated by a telephone call. The call is usually very early in the morning 6-7am (likely so the victim cannot call the bank to inquire) The scammer then tells the complainant that they are calling from XXX bank (BMO, TD, RBC etc..) and that there has been an unauthorized transaction on their account – a wire transfer to India seems to be the common theme in Saint John – the scammer then tells the person that they have to go to (Money Mart, Western Union…..) and transfer money to the scammer who is representing himself as someone from the bank. They are told not to contact their own bank (RED FLAG) but to meet a person – (name used is FRED RODRIGUEZ, PAUL RODRIGUEZ) at one of the local banks AFTER they have wired the money. A time and local bank address is usually given, however, the person will never show up because they had no intention of showing up and they already have the money.

- **If you find a suspicious or unauthorized transaction, report it immediately to your Financial Institution or Credit Card Company before contacting the Police.**

8. **Business Executive Scam:**

Sometimes referred to as the Business Email Compromise scam, this fraud starts when a potential victim receives an email that appears to come from an executive in their company who has the authority to request wire transfers. In some cases, the fraudsters create email addresses that mimic those of the CEO or CFO. In other cases, the fraudsters have compromised and subsequently used the email account belonging to the CEO or CFO. Often, the email will indicate that the "executive" is working off-site and has identified an outstanding payment that needs to be made as soon as possible. The "executive" instructs the payment to be made and provides a name and a bank account where the funds, generally a large dollar amount, are to be sent. Losses to this scam typically range from tens of thousands of dollars to hundreds of thousands of dollars.

- **Verify any email requesting wire transfers with co-workers and supervisors. Contact the source of the email to verify the request. Better to check first than check later, and realize you have sent thousands of dollars of your company's money to a scam artist!**

Have you been a victim?

- **You should report deceptive telemarketing to the Canadian Anti-Fraud Centre online or by calling (1-888-495-8501)**
- **If you suspect you may be the victim of fraud or have been tricked into giving personal or financial information, contact your local police service. (506-648-3333)**
- **If your social insurance number (SIN) has been stolen, you should contact Service Canada at 1-800-206-7218.**
- **If you think your CRA user ID or the password you use in personal dealings with the CRA has been compromised, contact CRA. (1-800-959-8281)**