City of Richmond 1st Quarter - 2022

CRIME PREVENTION

WORKING TOGETHER TO PREVENT CRIME NEWSLETTER

Protect Yourself Against Scams

Fraudsters are abusing the trust of their victims to steal information and money. While the scam may be old, the techniques fraudsters use are evolving. Be careful who you talk to on the phone and online as scammers use different methods such as spoofing phone numbers and phishing emails to scam you.

How to identify a Canada Revenue Agency (CRA) scam

- Unconventional Payments – Fraudsters may demand immediate payment such as pre-paid credit cards, crypto currency, gift cards, or e-transfer because they are generally unrecoverable.
- Aggressive Behavior – Scammers often use aggressive phrases to cause a sense of panic and scare you into sharing your personal information.
- Instant Messaging and Email – The CRA will never use text messaging or instant messaging to communicate with you. The CRA will only email you a link if you request it **during** a phone call or a meeting with them.

Romance and Crypto Scams—New Trends

- Fraudsters identify a person's friend and takes control of the friend's social media account. The fraudster will pose as the friend, convinces the person to invest or pay money to them.
- Fraudsters research their potential victims online, reviewing public social media posts and come up with a personalized strategy for each victim.
- Fraudsters convince their victim to invest into cryptocurrency and try to get the victim to provide remote access to their computer. They show them a fake website promising huge returns. Once they invest, fraudsters then cut off all communication with the victim and the money is gone.

Tips for dealing with CRA and Romance/Crypto Scams

- When you are unsure of who you are talking to, hang up, find the specific organization's number online, and call them back to confirm the call.
- Review your credit report at least once a year at Equifax and TransUnion and report any signs of suspicious activity immediately to your creditor.
- Be careful not to click on random links in any email you receive.
- Never send money or take investment advice from someone you have solely met online.
- Keep your social media accounts on private and beware of what you post online.
- Use a unique password and multi-factor authentication to secure your account and authorize transactions.

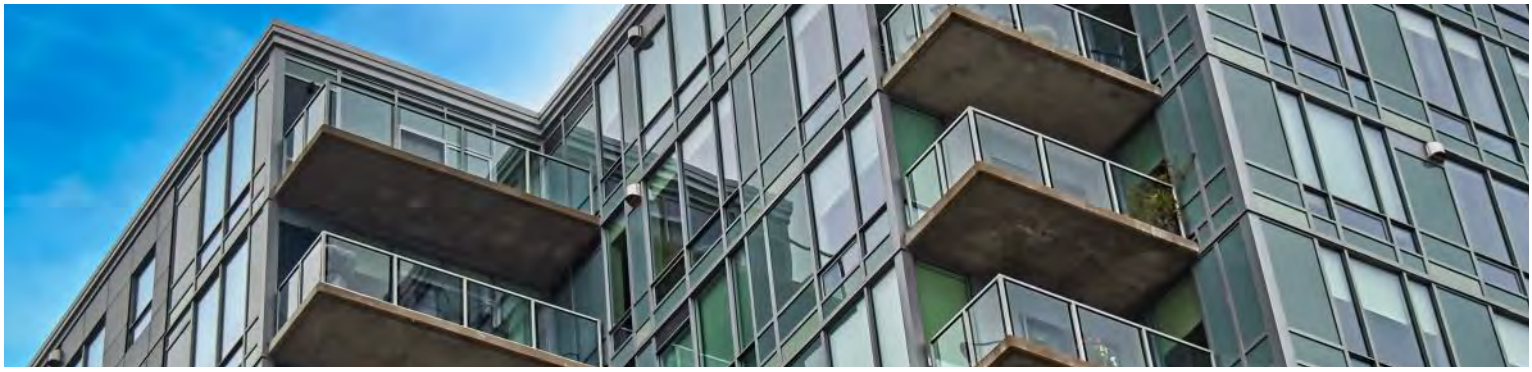
What to do if you are scammed?

If you are a victim to a scam please report it to the local police and the Canadian Anti-Fraud Centre (1-888-495-8501). Contact your bank and Service Canada (1-866-274-6627) to cancel and report compromised credit cards and stolen social insurance numbers.

CITY OF RICHMOND CRIME PREVENTION NEWSLETTER

Apartment dwellers often believe that they are safe from break and enters because they live above street level. Thieves however can still get into the building. Here are some crime prevention tips in keeping you and your neighbours safe:

- "No Key No Enter" - do not allow strangers to enter the building as you are leaving or entering. (You can get these stickers from us at Block Watch!)
- Make sure to change all the locks when you move in, as previous tenants may still have copies of the keys.
- Install additional locks to further secure your door, such as swing bar door guard, door reinforcement lock or chain door guard.
- Do not buzz people in without talking to them first. If you are not expecting a delivery or guest, ask for more information if your buzzer rings. Do not buzz anyone into the building whom you don't know.
- Always lock your door even if you are only stepping out to take the garbage out or grab your mail.
- Do not leave your keys in the door.
- Note the lighting of common areas such as storage and bike rooms. Ask for more lighting and security camera coverage if needed.
- When leaving the secure parkade, make sure the gate fully closes behind you before driving off.
- Report any poorly lit areas, overgrown shrubbery, any damaged doors and windows around your complex to the building manager.
- Remove all valuables and personal items from your vehicle. If you have to leave items in your vehicle, place them in your trunk.
- Never leave a spare fob in your vehicle. Especially not in plain sight.
- Always lock your vehicle and keep your windows closed before walking away.
- Get to know other people who live on your floor so you may be able to identify strangers.
- Collect your mail daily, never let your mailbox overflow.
- Install additional locks on sliding doors, especially if you live on the ground level.



Christmas Caroling Night

We had a wonderful time at the Christmas caroling event, hosted by our Block Watch group in the St Albans area. Despite the cold and occasional rainy weather, we had approximately 30 neighbours that came out to sing, along with Constable Chan and Corporal Wong from the Richmond RCMP Community Engagement Team.

It was a heartfelt experience as we saw their community celebrate the holiday season together even though they were all strangers a few months ago. The kids, adults, and officers chatted amongst themselves and the neighbours enjoyed the songs at their doors. We could feel the Christmas spirit through the joyful interactions of the community.

Thanks to the Block Captains for hosting the event, printing out song books, providing flashlights and planning the caroling routes. This event showed many people that Block Watch is not just a program but a family of neighbours. It is through these connections that make the community stronger, closer and safer.

To start a Block Watch Group

Interested in starting a Block Watch group? Let us tell you a little about Block Watch! Block Watch is a program that brings the police and the communities together. This program helps you build connections and relationships with people in your neighborhood and the police while striving for the common goal of crime prevention.

Select a Captain/Co-Captain

- ◊ Each Captain/Co-Captain must submit an application and complete a Police Information Check

Recruit and build your group

- ◊ Recruit homes that are near to you. To build an effective Block Watch, try to involve 50-75% of households in your area. We will provide you with recruitment packages.

Complete activation of your team

1. **Complete** Block Watch Captain/Participant training - Register as many of your group as you can for a virtual training session.
2. **Submit** your participating household list.
3. **Qualify** for Block Watch street signs once above steps are completed.

If you are interested in creating a Block Watch group in your area, email us your name and address at blockwatch@richmond.ca or call 604-207-4829.

BUSINESS LINK

WORKING TOGETHER TO PREVENT CRIME NEWSLETTER

Protecting Yourself Against Business Email Compromise

The Business Email Compromise (BEC) scam is an example of spear-phishing tactic that criminals use to steal and gain knowledge from a business and its employees. The term spear phishing involves a scammer pretending to be a legitimate source to convince employees to send money or share financial information. BEC scams are continuously evolving as it no longer just involves emails but also social media accounts such as Instagram or Facebook. Therefore, it is important to recognize BEC scams because many people are working from home and may not have the software or knowledge to combat cybercrimes.

How to recognize BEC scams

- Scammers demand payment in unconventional pay methods such as crypto currency or gift cards.
- Scammers often want their action done **quickly** and **secretly**.
- Double check email addresses and/or social media handles. Fraudsters may use spoofed emails or social media handles that are slightly altered.
- Check for grammatical or spelling mistakes.
- Be cautious with unexpected request for payments that do not coincide with normal payment schedules.
- Beware of requests that requires you to click on a link to get to a login page.

How to protect your business

- Educating employees on how to spot BEC scams is one of the best ways to protect your business.
- Update all anti-virus software on all computers, servers, and mobile devices.
- Confirm payment requests through another means of communication. Do not rely only on emails.
- Never open emails and click on links from unknown email addresses.
- Get “verified” on social media as it adds another layer of credibility to your account.

Report it

Whether you are a target or a victim to the BEC you should report it. Be sure to report the incident to your IT personnel, the local police, and the Canadian Anti-Fraud Centre. If funds were transferred, immediately report the incident to your financial institution.