



Monthly Update to Members of Cochrane Foothills Protective Association

**What to do ?**

One in three families will likely fall for a scam, phishing or other means of interpersonal online fraud each year. This applies to all of us. The Canada Antifraud Centre reports romance scams as recently being the largest losses. <https://www.ctvnews.ca/lifestyle/no-1-scam-romance-fraud-cost-canadians-more-than-22-5m-in-2018-1.4294076> This vignette has composite elements of several situations.

You have known your friend 'Terry' for several decades. He worked in senior management in the IT field. Recently he lost his partner of many years. He seems lost, wayward and in search of a partner. He spends time on dating sites. He shows a few friends a revealing picture of the focus of his attention. He says he is going to the airport to pick her up. He comes home alone. Several other times, he has gone expectantly to the airport and again returned - alone. He has a solid pension from many years of work. He downsized twice and recently moved into a basement of a friend. He no longer has a car. He avoids long standing friends and family. Police advise it is worth paying attention to, but they cannot investigate for probable fraud without his complaint. Looking at the materials on romance frauds, we see many markers. Recent grief. Lonely. Incremental commitments. High hopes. Embarrassed. Blames self. Does not tell anyone. Put off dealing with situation. So what should we do when someone you know gets taken in by a fraud? This is very delicate, critical and complex. **What will you do as a close friend or relative?** The extract below on romance fraud is from the Canada Antifraud Centre.



**Reject it: How can I protect myself or loved one?**

- Be suspicious when someone you haven't met in person professes their love to you. Ask yourself –would someone I've never met really declare their love after only a few emails?
- Be wary when someone you meet on social media wants to quickly move to a private mode of communication (email, text).
- If trying to set up an in-person meeting, be suspicious if they always have an excuse not to meet.
- If you do actually set up a meeting – tell family or friends when and where you're going and meet in a local, public place.
- Do not share personal (birth date, address) or financial information with anyone you've only just met online or in person.
- Never send intimate photos or video of yourself. The scammer may try to use these to blackmail you into sending money.
- Be cautious when conversing with an individual that claims to live close to you but is working overseas.
- Never under any circumstance send money for any reason. The scammer will make it seem like an emergency, they may even express distress or anger to make you feel guilty but DO NOT send money.

- Should you be asked to accept money (e-transfer, cheque) or goods (usually electronics) for you to transfer/send elsewhere, do not accept to do so. This is usually a form of money laundering which is a criminal offence.

If you suspect a loved one may be a victim of a romance scam – based on any above points –explain the concerns and risks to them and help them get out of the situation.

Links - <http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/romance-rencontre-eng.htm> and [https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-IBBS2-EN.pdf/\\$file/CB-IBBS2-EN.pdf](https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-IBBS2-EN.pdf/$file/CB-IBBS2-EN.pdf)

### **UNREAL Hang-up calls**

Our frequent access to multiple media leaves us with countless interruptions that may lead to an intrusion. For phone calls, how many do we get a week for credit card alerts and opportunities, surveys and solicitations? How many targeted opportunities are we sent on the internet? Never mind the blanket ads and fake information. We are awash in the widest array of materials designed to catch and keep our attention, get some interaction, and move subtly through increasing details and commitment towards something that is our purchase or loss. This is the normal tactic for broadcast online sales. The challenge is to sort acceptable messages from those where the intent of fraudsters is to use the interaction to steal. An example follows of the prevalent hang up calls scam.

A woman gets a call from her bank or the RCMP alerting her that her credit card appears to have several unusual charges. The caller suggests she check it out by promptly calling the information number on the back of the credit card. She calls immediately and the recipient on the phone line acts like a credit card call centre. She gives her credit card number and other identification information to verify her identity. The information gleaned is used to create a duplicate card and charge amounts. Messages – deal only with people you know at your bank.



Links to UNREAL hang up calls and how they work on landlines

<https://www.cbc.ca/news/canada/nova-scotia/phone-scam-bank-nova-scotia-victim-1.5192508>

<https://www.cbc.ca/news/canada/toronto/phone-fraud-toronto-1.4528233>

<https://www.cbc.ca/news/canada/calgary/bank-fraud-scam-landline-police-warning-1.5216547>

### **How awkward is this**



A well dressed professional has lunch in a busy food court. He leaves his jacket on the back of the chair. When he leaves a few minutes later, he notices his wallet is missing from the inside pocket of his jacket. He sets about calling the several credit card companies to freeze the cards. In the moments needed to find the phone numbers, make the calls and ask for a freeze on the card, twenty minutes has passed. In that time, charges were made on several cards for a total of

approximately \$38,000. The debit card was also used to withdraw the maximum daily limit. Then he started getting replacements identification and new cards. This is a long and tedious process as issuing institutions need to verify the loss, check identity and go through the internal procedures – all for our security. Banks resist debit card fraud as a PIN is required. Messages – keep cards and valuables on the person, beware of others in cues and note that organized thieves use networks to instantly disseminate and use credit cards. Check the monthly statements promptly and thoroughly.

### **Locally, recently. Continually?**

Vehicles were entered while parked outside. The garage was entered. The doors were not locked. In another case, thieves entered a vehicle in the driveway, and used the garage door remote to enter the attached garage. There, keys were removed from a collector vehicle. Expect another entry with keys to steal the collector vehicle?

In yet another case, a homeowner had the doorbell ring. A guy at the door said he ran out of gas and was looking for some. Apparently he went up and down the street with the same story, but told one person he "lived on a farm just around the corner". Eventually someone gave him some gas. They didn't get the license plate on the van.

And in yet another situation, the owner opened a utility shed to find gloves, a transaction notebook and several crystals of meth in a zip lock. The owner has no knowledge of the user of the space or when it happened.

### **RCW Mantra - ORR**

**Observe.** Really pay attention to all that is going on. Be cautious. Check out as seems reasonable.

**Record** as much information as possible. Pictures and descriptions of people and vehicles (make, model, colour, and license number) are valuable. Also important is the location where a situation occurs so a responder call is most efficient.

**Report** promptly to the RCMP. Call 911 or 403 932 2211 for the RCMP Cochrane. Even if you are in doubt, report it. Leave it to the experts to decide if action is needed.

### **RCW Participation**

Check out the news and links on our website <https://cfparcw.ca/>. Invite your neighbours to also become part of your community movement to send a message to would-be intruders. "Beware. These rural people are informed, prepared and connected to deter crime."



**Invitation to Members** If you have any information, comments or questions to share in the next newsletter, please submit to the general CFPA email address: [info@cfparcw.ca](mailto:info@cfparcw.ca) We are Rural Crime Watch, a network of concerned residents, committed to making a safer community through basic crime prevention principles. Our security is greatly enhanced when we work together as good rural neighbours.

Writer this issue - Jim Willson