

PROSTATE CANCER CANADA - NEWMARKET

Volume 16, Issue 2,

October 15, 2011

**A support group that provides understanding,
hope and information to prostate cancer patients and their families**

We all know that as we get older we don't seem to get enough exercise, Well, come to our October 20th meeting and hear what Daniel Santa Mina a leading Exercise Physiologist has to say about that. It will change how you view your Prostate Cancer future. Daniel holds a Cancer Exercise Specialist certification from the University of Northern Colorado. He has published two book chapters on exercise and prostate cancer and has presented his published research at national and international scientific conferences. Daniel currently directs the Survivorship Exercise Program at the Prostate Centre in the Princess Margaret Hospital in Toronto. Daniel will be discussing the importance of exercise throughout the course of treatment for prostate cancer.

Meeting Date: October 20th, 2011

Place: Newmarket Seniors Meeting Place,
474 Davis Drive, Newmarket

Time: 7:00 pm to 9:00 pm

Speaker: Daniel Santa Mina, Exercise Physiologist

Subject: Exercising as a treatment for Prostate Cancer

Prostate Cancer Canada - Newmarket
Newmarket, Ontario. 905-830-0447
www.newmarketprostatecancer.com

a member of the



Assisted by the Canadian Cancer Society
Holland River Unit
Cancer Information Service
1 - 888 - 939 - 3333

Your Executive

Frank Kennedy, <i>October Host,</i>	905-895-2263
Ulli Baumhard, <i>Greeter,</i>	905-478-8843
Phil Mahon, <i>Secretary,</i>	905-473-2688
Ron Stevenson, <i>Treasurer,</i>	905-836-1701
Jane & Frank Kennedy, <i>Newsletter,</i>	905-895-2263
Pat & Ron Stevenson, <i>Greeters,</i>	905-836-1701
Dan Ho, <i>Member at large,</i>	416-953-8889
Murray Green, <i>Member at large,</i>	905-830-9753
Doug Bowers, <i>Member at large,</i>	905-841-2759
Doug Armstrong, <i>Member at large,</i>	905-778-0028
Walt Klywak, <i>Member at large,</i>	905-895-1975

The Newmarket Prostate Cancer Support Group does not recommend products, treatment modalities, medications, or physicians. All information is, however, freely shared.

September Speaker notes . . . Detective Constable, Andrew Quibell and Detective Constable Ian Mason

Subject: Fighting Senior Fraud



Detective Constable Andrew Quibell and Detective Constable Ian Mason talked to our Support group at our September 15 meeting. They both work with the Major Fraud Department of the York Regional Police. The York Region Fraud Department is made up of three different sections. There is a Corporate Section, where they investigate Ponzi Schemes and big corporate investigations; there is a General Team, that detective Ian Mason works with and deals with seniors and grandparent schemes and cheque frauds; Detective Andrew Quibell's team, the Card Team, debit cards, credit cards, is where they investigate point of sale terminal cases and ATM skim cases. During their presentation they shared their experiences, often answering the same question with anecdotes from their own cases. Here is what they had to say. What we investigate is fraud and fraud is when you deceive someone or mislead them. In the card fraud business, the majority of people we deal with on my team are young, male suspects between the ages of 18 and 30. Most of these suspects are members of organized crime groups. The technologies available to people today make this easy for them. There are on-line sources that sell the equipment they require to set up a lab, which can be done with a laptop at this point. There are several different groups that we deal with that are involved with fraud and the profits made from the frauds. There are several types of frauds. The incidents of most interest to yourselves and people that are related to you, as well as friends, are the skimming of debit and credit cards, as well as identity theft and internet frauds and telemarketing and mail frauds. Other incidences involve contractors and sales persons, and also investment frauds.

The good news is, seniors aren't typically privy to too much of the identity thefts, because, obviously, you have to take on someone's identity. A lot of the people who are doing frauds are the younger people. So just by that alone it's going

to take you out. What I've noticed a lot is contractor frauds. A lot of seniors seem to be taken advantage of in these situations. They offer to work at your house and then they do a poor job. That in itself is more of a civil issue but, if they are doing it to multiple people and they seem to target the same groups all the time, they typically don't get reported, that then becomes a fraud. There are a couple of others: there are power of attorney family frauds. Unfortunately and we don't like to talk about that because it's very embarrassing personally to us, when our families are taking advantage of ourselves. All of a sudden they are power of attorney on my stuff and they are selling it. Saying, "Oh, my grandparents, my parents, are losing it so I need to do this. They are convincing the powers to be that they are your power of attorney and the next thing you know, all your money's gone. Everyone's fine, everyone's good but you're getting taken advantage of by your own family, which again goes unreported. So those are basically the topics you're going to find that are more prevalent with our retired community.

I want to show you how easy it is for someone to commit what is called a point of sale terminal or impact theft. At any convenience store you can simply swipe your card to complete a sale. These pin pads are regularly being stolen. This is a huge problem across York Region and the GTA. There are three reasons that they do something like this. One is new technology and they want to learn how the technology works so they can copy it; two, they want to take it and place it somewhere else in place of another one, as a decoy; three, the usual reason is that the device they are taking has already been tampered with. It has some sort of a recording device inside of it. It's transmitting and they are taking the data of the customers with them and from that they are able to create game cards with that data and then make transactions with your information.



- Q.** Are you saying that they are switching with another one?
A. Yes, what we are dealing with are pinpad thefts and

there are pinpad tamperers and switches. What happens is, towards the end of an evening, the suspects will go into a business, they will remove the pinpad and replace it with another pinpad. They go home with that pinpad and they tamper with it and put a device inside it that is capable of capturing data. The first thing the next morning, they go back to the store again and replace it and now they have a tampered pinpad in that business. Usually these people work in an organized group. So, the staff will be busy working with another one of these individuals, unknown to them, usually in busy places where they are able to get away with this type of thing. The other thing with is that they are now able to sit in the parking lot and it transmits and sometimes they don't even have to Øo back in.

Q. Are the chip cards correcting this problem?

A. Chip cards are a different thing. They started in Europe and the Europeans had a chip card technology which they are now having some problems with. In Canada, we have a newer, better technology but the United States have been resistant in joining us. The problem we have now is that you've got American cards with no chip. The other issue we have is that there are different deadlines leading up to the compliance stages for our merchants. For example: I have a chip card. When I use my chip card, what should happen is, I should go to the store to make my purchase and put the chip card in, basically in the bottom of the machine and, when I do that, I then put in my pin number for my chip card. So all the data is running through the chip. It's a two-step security feature. You have the chip and the pin number. Where we are at now, because we are at the stage where we are not fully compliant yet, some businesses are still working on the magnetic strip data. So, even if you have the chip card, if the merchant puts my card through with the mag data our chip has now been defeated because it was not used properly. What we rely on is the merchants to use the card as it was intended, which we are getting close to.

Q. We have merchants who do not have the capability of doing that.

A. They are now being forced to do it. It's coming very close now. These are expensive units, so there are a lot of people holding out. The smaller business man is saying that these cost a lot of money and he can't afford to do that now. So he is going to wait until the very last minute until he has to. What they are doing is saying unless your company has this chip compatibility through the insertion of the card by a certain date then, you're cut off. The trouble is that they are still able to do it until that cut off comes around. Because you still have the mag. strip on the card, some people on the inside might say that the chip isn't working so they have to swipe the card, which enables them to get your information. There has still not been a single reported case of the chip being compromised. However, a chip card which has been swiped has been compromised because of the mag strip on the back. If a clerk says that the chip isn't working and you

should just swipe it, that's a red flag. Tell him I would like try my chip again. I was in a meeting with these officers and I know there's a lot of fraud going on and I don't want to swipe it. Just make yourself aware and be informed.

Our suspects are very mobile individuals. These people will get in their car and drive from Toronto to Montreal in a day, just as you would drive to your grocery store and back. They think nothing of driving five, six, seven hours and in a lot of cases, as they are going from Toronto to Montreal, they are making a stop in Oshawa, Port Hope, Belleville, Kingston and onward, committing crime as they go, all the way to Montreal and all the way back, with your card, potentially. What's happening is, there are all types of fraud, everything from ATM skimming to pinpad tampering. The challenge with that, and where we've really done well in the past couple of years, is in our communication within our key services. Because we all have boundaries. The fraudsters do not. So we have opened up our communications with fellow officers across Ontario and across Canada.

We share our information and that's how we're gaining ground on these individuals. With ATM fraud, the machine is usually in a vestibule just as you enter your bank, or the newest thing is the drive-through ATMs. The drive-through are more susceptible to fraud, what they'll do sometimes is pull up beside the machine in their van and within a matter of 10 seconds they will install their overlay.



An overlay is a two-step process. You have a pin hole camera which will go above and then the device to put your card in. What happens when you insert your card, it captures the data from the card including the date and time, and with the pin hole camera they are now capturing your pin number. What we suggest is when you go to an ATM, grab hold of the unit where you insert the card and pull on it. If it comes off, there's a problem. They use an adhesive or double sided tape, quick and easy. It will come off if it's a fraudulent overlay. Generally what happens is these individuals will put these on for a matter of a couple of hours. They will generally be in the area watching and once they have whatever number of customers they deem to be enough, they will go back and remove the devices and they'll use that data to create their own cards and make transactions with those cards. There are

all different levels. We've got guys whose job is to create these false overlays. We've also got technicians whose job is to figure out the wiring of the pinpads, how they operate and how they work. It's almost like a game of chess. Every time we come up with something, they come up with something new and vice versa. Always be aware of this, don't hesitate to give it a good pull. Another technique that we've found used by these individuals is, if there's more than one ATM, sometimes they will jam something into the slot of the ATM to disable it and direct you to use the ATM that they've tampered with. We've found some of them right in Newmarket. Don't confront these individuals if you come across them it would be better to get a description of what they look like, get a plate number, call it into the police and let us deal with it. Surely we want to know about this and we have officers on patrol in all different areas of Newmarket and surrounding areas and they will deal with these people. Q. What about those machines which are in stores and gas stations, etc. which aren't affiliated with a particular bank? A. We call those a white label machine in the industry. What that means is that ATM which you'll find in gas stations, bars, restaurants is not affiliated with any one financial institution or bank. It's a private company that stocks the money and so on, those are organized crime. That's exactly what it is — organized crime that runs them and most of them in our area are white label machines because they are not monitored the same way that your regular ATM is. My advice would be not to use one. They are more easily tampered with and cause a lot more problems.

If you have a choice of using a credit card or debit card for a transaction, my advice personally would be to always use your credit card, simply for the fact that a debit card is an instant transaction. Once you make that transaction, the money's gone from your account whereas the credit card, until you receive your statement and pay, it's still the credit card company's money that is on the line. Another thing we find a lot is traditionally, when you go to get your gas, a lot of times there are issues with the gas station attendants, who are creating problems with fraud. This is still happening. One case that happened in Vaughan just recently: A young gas station attendant had a card reader in his pocket. Someone would come in with a card to make a transaction, the attendant would swipe it through for the regular transaction and then keep holding it below the level of the counter and quickly swipe it, again in this pocket reader, it's that easy. He could also have it close to his Blackberry and transmit information to a guy in the parking lot. Before you're even out of the place, he's withdrawing money out of the ATM across the street, that's how fast it can happen.

Q. What about the readers at the gas pump itself?

A. They used to be safe, now we're finding that those are also being tampered with. The issue with that is, in order to access the interior panel of the gas pump, they have to have some knowledge of that pump and an inside contact at

the station to turn off the video camera when they are tampering with the device.

Office Andrew said that there all kinds of interesting things that we come across. I love my job. I love the fraud unit. Everyday there are different kinds of investigations. We work sometimes with CBSA, which is our Customs Enforcement people at the airports. What we do is what's called a controlled delivery. Somewhere else, maybe Asia or Eastern Europe, someone will send a package. For example, one case was a box of tea. Inside that box of tea when you open it up you'll find 500 credit cards. A lot of times they will go to great lengths to disguise these credit cards. For example, one says Future Club on the front of it. When you peel it back, what it is, is actually a Mastercard. There are several stages to having a fraudulent credit card. When you've got the right plastic cards, you need to have an embossing machine to put the name and the number on the card and also the mag. strip data and then you've got an active credit card. It's that easy for them to do this. Because they have all the right tools to do it.

Q. How concerned do we need to be when we give our credit card number on the phone for over the phone purchases, where they ask you for your security code on the back?

A. I would personally want to know whether it's a reputable company, like a Sears or Canadian Tire and that I have contacted them and it's not someone soliciting a sale and asking for your information. It's important that you have contacted them and they are not contacting you, then it's usually O.K.

Q. What about selling something and getting paid through Paypal?

A. You have to be really careful with Paypal. I wouldn't be sending anything by mail or UPS until you have been paid and the money is in your bank. In the case of selling something to someone, until you have cash in your bank and it's been approved. Say, "Thanks for buying it. As soon as you have the money in my bank, I will send it to you." I do want to qualify Paypal - it's not that the organization itself is defrauding you but they are not protecting you from others who use their name to defraud you. I would also be very cautious about E-Bay or other International organizations, if you are buying something outside North America over the internet. Not to say that there aren't honest people all over the world, because there certainly are, but this is also an opportunity for a person in another part of the world to take advantage of you.

We also have problems with fraudulent SIN cards, drivers licences, passports and health cards. We have recently had a lot of success with executing search warrants and arresting certain individuals in different parts of the world, who are responsible for running document labs in York Region. For example, during one investigation, we determined that one rural address just north of Newmarket had 78 Ontario Driver's Licenses registered at that address. To me that's a

big problem. There's no way that should happen. That's something we're addressing through the Ministry of Transportation and hopefully a remedy is coming soon.

Q. What should you do with those cards, SIN cards?

A. They're not of much use, are they? Keep them at home locked in your safe. Do you know your SIN number. How often do you have to use it? I can't remember the last time I used my SIN number. Maybe if you open up a bank account. I know you need it when you're paying your taxes, but they can use that information along with a fraudulent Driver's license: two pieces of government identity, to open a bank account in your name. Put some deposits in there. Make some withdrawals. They could assume your identity and that, of course, is what is happening. It's a huge problem. If someone has your identity, they can open a line of credit in your name.

If you get an e-mail or a call from someone who identifies themselves as your bank, there's a problem. Banks don't send you an e-mail and banks don't call you asking for your personal information. They already know that. This is someone trying to gain your information and your trust. Unfortunately, it happens very frequently. As a result of all these things happening, everyone is paying extra service charges, everyone's paying a higher interest rate with credit cards. This is all a result of the fraudulence. We are talking about billions of dollars.

One issue that we've had in York Region, in the Vaughan area, we did an investigation with Canada Post. They have their own security personnel who are excellent. They had some concerns about one of their carriers, so we spent one day following this carrier on his route. When we decided we had gained enough evidence, we arrested this individual and what we found was that he had 32 envelopes tucked inside his waist. What he had done is, at the beginning of each carrier's route, they have to sort the mail. He wasn't just sorting the mail for his route, he was checking the mail for other routes, knowing what they contained. What we found was that the 32 envelopes contained \$128,000 in business and government cheques for one day. You are looking at the possibilities of massive amounts of money going to the wrong people and effecting all of us. This is going on every day. Again, any time you have financial documents and you are finished with them, if you don't have a shredder, I would suggest investing in one. Financial information in the wrong hands can be devastating to you. As well, these individuals are not below going through your garbage, they'll do that. When you put out your garbage, it is no longer yours. Anybody can take it because you have gotten rid of it. If you use a computer, consider getting some form of protection for your computer. There are always viruses out there. I am a huge hockey fan. There was one hockey website I used to go to because they always had good information. I accidentally got a virus from it and it was a huge problem. Just be cautious and get protection for your computer.

If you receive an e-mail or a phone call from someone claiming to be a relative of yours who is in trouble, you have to be very cautious unless you entirely recognize the person's voice. You don't want to commit to anything or provide any financial information. You should also contact another relative to confirm the information from that caller. Or you could ask them some information about your family that they should know if they are who they are claiming to be. A common trick is for someone to claim they are your grandchild; they are in trouble but don't want to upset their parents; will you bail them out so that the police will let them go home? They may even have someone else there acting as a police officer who will corroborate their story and will direct you how you can send the fine or bail money. This is a full time job for a fraudster. He will spend all day on the phone, making hundreds of phone calls, until he can find someone who will fall for it, getting upwards of \$5,000 from an unsuspecting "grandparent." Then he will go on to the next one.

Unfortunately, they say that only 10% of fraudulent activity is ever reported. That goes for all age groups, all frauds. Specific to this type of grandparent scam, or emergency scam, they are talking about only 1% are reported. There's been almost \$100,000 in personal losses in York Region this year so far. So, if there's only \$100,000 that have been reported, that's a heck of a lot of money from our senior population. There was a case of an elderly lady living in the senior apartments at Lorne and Davis in Newmarket. She helped her "grandchild" with \$3,000. That's a lot of money for me and I am earning money every week. She's an 81 year old on a pension, that's a lot more for her. This is very difficult for us to try to solve. We don't have any concrete information regarding phone numbers or locations. If you are unlucky, if you've been victimized, the only chance we have is if we have the location of where the money is picked up and, from here, that is usually Montreal.

Halton Regional Police just made a huge arrest. They found one of these boiler rooms in a house. It was a specific cell that was working, doing the phone calls and collecting the money. Eight or ten people were arrested. I talked to the investigator because I thought that maybe these guys were responsible for some of my victims. The guy I was on the phone with said, "Sorry, buddy. All the victims were from south of the border in the States." This is from Oakville, this is where these guys were arrested. They were responsible for about \$13,000 a day. It goes on everywhere. There's something that's going to be coming on in the next few months and most of them should be slowing down after that. You'll read about it in the newspapers. Being a victim is nothing to be embarrassed about, which is a natural reaction. People think, "My kids are going to take my power of attorney because they'll think I'm a doddering old fool." That's what I hear from a lot of people. That just isn't true. They're victimizing people. They're expert at doing it. They're good at it. It frequently goes unreported and that's what happens to a lot of the fraud

cases. You have to, have to, have to report it, otherwise we're not going to find the guy who did this to you.

Q. What is this star57? Is that a trace? It's very new to my mind.

A. It's actually in the front of the phone book and it's been there for years and I don't know why it's not more well known. I think it's one of those necessary evils for Bell Canada that they have to have it. What it does, basically, if you get a phone call. Usually it's good in harassment cases. As soon as you hang up the phone, you pick it up again, get a dial tone, press star57 and it tags, puts a marker on that phone call, gives it a little flag to make it easier for Bell Canada to trace.

Another safeguard, when you think of it, when you

can, you should consider reviewing your credit card statements to make sure that all the transactions are ones that you made. A lot of times that's what's happening. People are using your credit card to make other purchases. That's one way of catching it. As well, if you're going on a trip somewhere, you should inform your credit card company so that they know that there's a reason why those transactions are happening where you are vacationing. You don't want to get down there and have them put a stop on your card. Which again, is a good thing that they are keeping track. Another thing you need is to keep track of your credit. If someone is using your identity with a lot of false transactions, that's affecting your credit rating.

In keeping with the message that our speaker will be focusing on at our October 20th meeting, here is a report from a Jane Maher a prominent United Kingdom Oncologist.

Exercise acts like a wonder “drug” for survivors

Regular exercise can cut by 40 percent the risk of cancer returning, say experts. Breast cancer patients who work out have more than a 40 percent lower risk of dying while prostate cancer patients 30 percent.

Exercise acts like a wonder “drug” for survivors of some forms of the disease, according to Macmillan Cancer Support. Physical activity should be “prescribed” by doctors after it was found not only to significantly help recovery but also prevent other long-term illnesses, the express.co.uk reported quoting the British charity. Some cancers have high cure rates but others can return years after they were first treated.

Rather than patients being told to “rest up”, doctors should encourage them to get moving as soon as they feel able, researchers believe. A review of more than 60 studies for Macmillan found that being active did not worsen people’s fatigue but had positive effects on their mood and well-being.

Once treatment has finished, exercise can reduce the impact of side-effects, such as swelling, anxiety, depression, fatigue, impaired mobility and changes to weight. Women with breast cancer who exercise for two-and-a-half hours a week at moderate intensity have more than a 40 percent lower risk of dying and the disease returning compared with those who do less than one hour of activity a week, researchers said. Prostate cancer patients have a 30 percent lower risk of dying from the disease and a 57 percent lower rate of disease progression if they exercise for three hours weekly.

Oncologist Jane Maher, chief medical officer of Macmillan, said: “The advice I would have given previously to my patients would have been to take it easy. “This has now changed significantly because of the recognition that if physical exercise were a drug, it would be hitting the headlines.”

“There really needs to be a cultural change, so that health professionals see physical activity as an integral part of cancer aftercare, not just an optional add-on,” Express quoted her as saying.