Rotorua SeniorNet

# Newsletter

February 2023

www.rotoruasenior.net

Member of NZ Federation of SeniorNet Societies

Postal address: PO Box 2090, Rotorua 3040 Phone: 022 6879299 Email:rotorua@seniornet.nz

## Contents



**Editor contact**
rotorua@seniornet.nz

**Website**
www.rotoruasenior.net

## From the Chairman

Hello, members

I trust that 2023 is treating you well.

The first major event of our year is our AGM at Parksyde at 2 pm on 13 February. While most of our officers and committee are willing to continue for the coming year, several of us are now in our 80s, and we would dearly like some younger blood. You do not need to be an IT expert, as there are organisational and social roles where we would appreciate support.

We had indicated that we would be seeking volunteers to help with the census, but it seems now that our role will be limited. SN's formal contribution will be to have SeniorNet learning centres as "Assisted Completion Locations". As we in Rotorua do not have a physical learning centre, we will not be participating in this way. However, if you need personal help with completing the census online, you can visit us at our Monday morning drop-in sessions at the library.

We will be running another series of our Talking Tech sessions at Parksyde on the 1st and 3rd Tuesdays of March, April, May, June and July – 10 sessions in all. As in our previous series, the main focus will be on getting the most from your smartphone. Because of support from Age Concern, we are able to offer these sessions at no charge.

Lastly, a tip. Back in December, our domain host advised that our automatic subscription payment had failed. Despite repeated attempts over many hours since to update our card details and pay online, I always got messages to "try again in a few minutes". A few days ago, in desperation I opened their website via Microsoft Edge instead of Google Chrome. EUREKA! It all worked. So, the tip is to try a different browser if all else fails.

Regards
Keith Garratt
Chair

*Rotorua SeniorNet is just one of 75 local groups in the New Zealand Federation. If you would like to know more about what goes on elsewhere, OR what discounts or services are available to members, go to the Federation website.*

*www.seniornet.nz*

# AGM
# Monday 13 February 2023
# Parksyde 2 pm

New volunteers willing to work with the committee are welcome. Technical skills are not necessary – for instance, we could use a social secretary (or similar title) who would be happy to help organise the social side of our activities, significant birthdays or other achievements, etc.

---

**From Bert, Activities Co-ordinator**

During the past few weeks, I have noticed a number of stories appearing in the media about telephone fraud and scams in which the victims were from the Senior population. Many of these were very sophisticated, plausible scenarios. Many of the victims were retired business and professional people whom one would think, in hindsight. would be the least likely to be taken in by such a seemingly obvious scam. However, the people who are developing these scams have been using them for many years in some cases. The scams have become very sophisticated. The bad guys have refined them over the years by abandoning what they have discovered does not work and polishing and perfecting what they know does work.

At home we still use a landline. We get regular calls from Visa telling us that our Visa card has been used for purchases from companies we have never dealt with. It is the same recorded voice each time and I simply put the phone down without speaking and let them waste their time. After a minute or so I check that they have broken the connection and hang up. I do much the same thing with calls from any mega company. We have all experienced how difficult it is to contact any large organisation by telephone. It can take a long time to actually talk to a human being. This would suggest that the odds that one of these organisations would take the trouble to contact you personally are infinitesimally small!

Recorded messages are, for most of us, just an irritation. The real danger lies in personal calls where someone you do not know phones you on some pretext or another to offer you an investment opportunity or pretending to be calling about your bank account or whatever. They want to engage you in conversation to glean as much personal and/or financial information as possible. These days I am very cautious about people I don't know asking me questions on the phone. I no longer respond to phone surveys for this reason. A huge red flag for me is when someone advises me to take a course of action online which will protect me from financial loss or missing out on a financial opportunity. These people can be very persuasive and sometimes start asking for small amounts which will slowly escalate once they have people hooked.

A recent development is that people are asked to buy gift cards in small denominations and pass them on to the scammers who promptly turn them into cash. All this is in the

pretence that it will protect their money which they have safely stored in a bank account. This leads me to the next subject which I feel needs a little clarification … Many people are reluctant to use internet banking! A little history here to explain my thinking on the advantages of using the internet to operate a bank account. My first contact with the banking system was when I was around ten years old and it was my job to walk up to our local Midland bank with the week's takings from Mum and Dad's shop. It was not a lot of money, but most people would take very little notice of a child of that age in a bank. They might surmise that I would be topping up my weekly savings from my pocket money and errands. I got to know the tellers and was fascinated to watch them swiftly count the notes and small change and enter the amount into a ledger and hand me a receipt.

As I grew older and learned a trade and earned a decent wage I had savings and a cheque account. The next step after getting married was negotiating a mortgage to purchase our first house. That was really grown-up stuff which was all part of my financial education. All of this was well before computers were commonplace.

Fast forward to the future. Personal computers and the internet changed the banking system forever. The paper ledgers used by the tellers of old were replaced by computer programs that recorded every transaction that each customer made with the bank. People still went to the bank branch to pay in cash amounts and present cheques and make withdrawals and make savings deposits etc. Soon it became apparent that sufficient numbers of people were using the internet and it was possible to do all of those things and much more online. The banks were quick to realise that the numbers of customers visiting the branches were dwindling rapidly and took the opportunity of divesting themselves of many valuable bank properties which were no longer required. They reinvested the proceeds of selling banking premises in software and hardware to build an extremely efficient online banking structure. They reduced the number of tellers and they retrained the remaining ones to be computer literate which made them individually much more productive. No more endlessly counting bank notes and coins and entering numbers into a ledger.

A very real consequence of all this was the demise of the cheque book recently and a significant drop in the amount of paper money and coinage in circulation. The internet has instead expanded the numbers of ways we can make payments. We can pay using internet banking on any of our devices. We can make payments on our phones using specific apps such as Google pay or Android pay. We can use our credit and debit cards by swiping using a pin number and Paywave which operates with a pay amount limit. The payment system has become fully automated and has been integrated into the banking system. This has allowed the banks to track the movement of money which has no reality except as numbers in an electronic ledger. The speed of these transactions is measured in nanoseconds. Every transaction can be checked and cross checked by running them through sub programs written for this purpose.

Banks realised very early in the process that all individual accounts needed protection from outside interference. All accounts are protected by a strong password which some banks require to be changed every quarter. Each account holder has a unique username so the bad guys need to discover a user name of indeterminate size and a password of

indeterminate size requiring millions of combinations which is changed on a regular basis. The almost universal use of the mobile phone has enabled the banks to introduce two factor authentication. When a transaction amount is above an agreed figure the bank's computer sends a message to your mobile phone which is a randomly generated one-time numeric password. To complete the transaction, you are required to type in the number supplied. Mobile phones can and should be set up so that only the owner has access. Most mobiles sold nowadays can be set up with fingerprint authentication coupled with a pin number. Also in the pipeline could be the use of facial, iris or voice recognition.

To all of those of you out there that are still hesitant about internet banking I would suggest that banking has never been safer than it is now. Human error at the bank has been reduced to a minimum. Customers can develop a few safety habits such as cutting and pasting bank account numbers from the supplier's invoice when making a payment to eliminate transcription errors.

Read the submit page carefully before pressing the submit button . To those who are not using this facility I would recommend paying a visit to your bank to at least discuss the possibilities. Banks will often offer assistance and training. SeniorNet can also provide you with any help you may need.

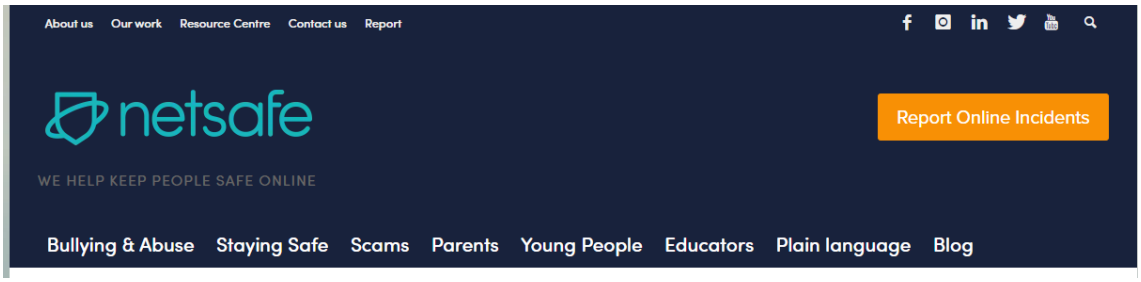
Bert Harris

## **FYI/FYE** (For Your Information/From Your Editor)

**netsafe.org.nz**

With the new school year starting, this seems like a good time to have a look at NetSafe. A lot of people think that this is for schoolchildren, but if we take a closer look, it is aimed at almost anyone, with options for subscribing (free!) as a parent, educator, online professional or general reader.

It is possible to download online, print or video forms of information, such as tips for staying safe online. The illustration below shows the main header for the website and the various pages that can be accessed.




This is a site that is well worth spending some time browsing. Remember, as long as you don't download, save or bookmark, you can just leave the site without any problems. And, of course, this applies to other sites – only save or bookmark them when you are sure you are going to want to use them again.

Considering the apparent prevalence of online stalking, bullying, identity theft, etc nowadays, a site like Netsafe can be very useful and not just for one age group. Those who have young relatives could find this even more valuable. If this newsletter reaches you in time, you might like to look at the event below, which is recognised by over 150 nations.


---

**And a further contribution from Bert** – an example of an attempted scam:

**First email:**

*On Fri, Jan 27, 2023 at 9:31 PM Margaret Berry <da.woods@ntlworld.com> wrote:*
*Hi,*

*Hope all is well? I'd like to ask you for a favour. Kindly, let me know if you get my email? Many thanks*

*Margaret*

**Second email:**

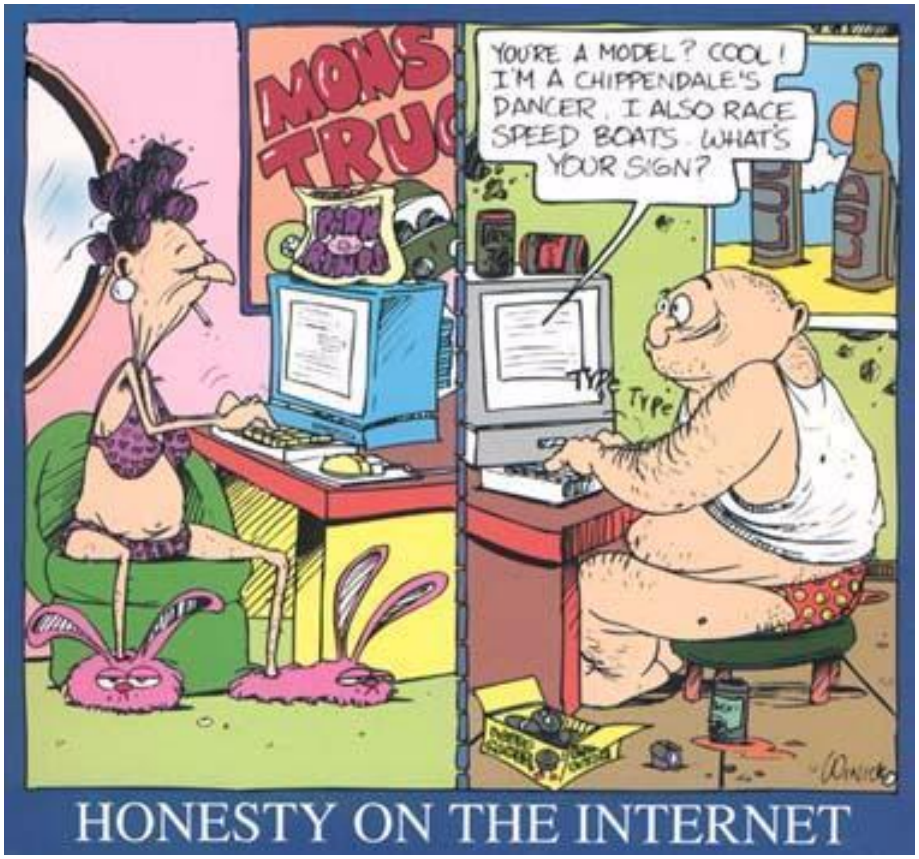
*On Sat, Jan 28, 2023 at 9:58 AM Margaret Berry <m.jberry@hotmail.com> wrote:*
*Glad to hear from you, I need you to get an Apple gift card for a friend's daughter who is down with cancer of the Liver, it's her birthday today and I promised to get it for her today, but I can't do this now because all my effort purchasing it online proved abortive. Can you get it online for her on my behalf? I'll reimburse you back as soon as possible. Kindly let me know if you can handle it.*

**Suspicious indicators:**

- Urgent sympathy demanding scenario.
- Request to purchase something that is readily available.
- An offer to reimburse.
- All this in an unsolicited email from an unfamiliar name.
- Different email addresses

So, how does it work? The person being scammed goes online, buys the gift card and emails it to the scammer. They have a free gift card to spend and never reimburse the person they've scammed.

**Always** look at the email address, read carefully and if in doubt, delete, block, etc. Remember, you can notify Netsafe.




**Committee and Tutor Contact Details**

| | | |
|---|---|---|
| Chair/Webmaster | Keith Garratt | 07 357 2020 |
| Vice Chairman/Treasurer | John Somerville | 021 181 5193 |
| Secretary | Peter McKellar | 07 347 1154 or 027 2216275 |
| Committee member | Rob Grant | 07 345 4222 |
| Committee members/tutors: | | |
| | Gene Rigney | 027 5724363 |
| | Bert Harris | 343 7232 |
| | Eric Cameron | 027 4410567 |
| | Len Watson | 07 345 4145 or 027 2636222 |
| | Felix Hohener | 021 737694 |
| | Alan Armstrong | 07 349 6344 or 021 171 0946 |

**THANKS TO OUR SPONSORS**