RCC | Redcliffe Computer Club

NEWSLETTER September 2021

Report from your President

Welcome to Spring!! Winter is behind us and we are promised a warm wet spring. Be interesting to see if the boffins are correct.

Well, Covid is still causing much heartache and problems for us all, one way or another. Let's hope we can get enough of us vaccinated to allow more freedoms in the near future. It is certainly impacting most businesses one way or another. Be a shame to see many go broke as a result. We are expecting the delta strain to make its way into Qld sometime soon and maybe create further lockdowns here. We will once again be forced to close down if and when that happens until such time as vaccination levels are acceptable.

On the bright side, we have seen an increase in club membership and have broken through the 300 membership mark for the first time!!! Great to see so many people getting help in this digital age. I'm sure that there are still many folk who are unaware of our services. Please tell anyone you meet who might be interested about our club and its purpose of helping in the digital age. Our club is open to all – not just seniors.

Many are still having issues with the installation and use of the Qld Covid app. We are quite happy if you call in anytime for a free 5 minute help with same. It is important to be able to use it.

More members have taken advantage of our laptop purchase and we still have some left for those interested. They are very good value.

Peter Emmerson is still away but Natasha is due to return early this month.

Our workshop on Zoom and other video chat systems is now over. We are planning one on Genealogy and another on Android phones and tablets in next few weeks. I'll advise dates for these in due course. They will both be popular so be quick to book when available. We are limited to 20 people each session but can repeat a session if enough are interested.

Be careful of a new scam running around. It comes as an sms message on your phone telling you that you have missed a phone call and suggests that you open a web page listed. The spelling is often really poor. Please do NOT try to open that web page. Just delete the message immediately. If you have really missed a phone call, it will be listed on your phone as a missed call. Be very aware – there are lots of baddies around.

Windows 11 is not far away. Seems will not be available on older computers due to security issues. Windows 10 will be supported by Microsoft for a year or so after Windows 11 is released.

All for now. Enjoy spring before the heat arrives again....

Ian Stewart - President.

Passwords

Passwords are one of the frustrations of modern life. We all know that they are important – like locks on our houses and cars.

And you don't realise how important they are when all of a sudden, you have to reset a computer or device and need to know that password.... In fact just about everything you do on the internet requires a password to create an account – whether it's email, Microsoft, ebay, your banking, or simply wanting to log onto an online business.
When repairing computers and devices, it doesn't matter what the device is, around 90% of people don't or can't remember their passwords for all their online activity. Some believe that they don't have a password at all because their device or computer web browser will store those passwords so that you never have to remember them. It is so important to have all your user names and passwords stored safely.... Even if it's a $2 address book from the dollar shop..

Here's a tip.. write your user names and passwords in pencil so you can easily erase an old password and replace it with a new one.... And of course keep that book in a very safe and secure place.
More importantly, you should also update these passwords at least every 12 months.

So what about passwords – do you go for convenience or security? If you have the same key for every account, you're in real trouble if you lose it or if you are hacked because you have just made it so easy for someone to hack all your accounts. – but having to remember a big bunch of keys and then find the right one can be a real pain....
Making your password your birthday is easy and convenient – but not secure.
Remembering 8 to 12 random characters including numbers and a mix of upper and lower case is much more secure, but hard to remember unless you're Rain Man..

But did you know that as well as guessing, you might use your date of birth, hackers have programmes that just run through every word in the dictionary to access your secure areas?
And to make things worse, because we can't remember 20 different words we tend to use the same word for all our passwords – which means once the bad guys succeed in one place - they can use your password everywhere...

Using children and grandchildren's names is also not a very good solution. I had one client that used the word "password123" which can be hacked in seconds.

The best advice I can give is use non-descript numbers and letters at random (both upper and lower case) and in some cases, web accounts will require symbols such as $, # and & as part of the mix for a password.
There are also many websites that will help you generate passwords completely at random. One such website is https://passwordsgenerator.net/ ..... easy to use, plenty of choices regarding upper and lower case, symbols, numbers etc. This website is safe and secure and once you have generated a password of your choice, the website destroys the password suggestion – just make sure you have written it down before moving on.

So, here are my tips for passwords:
To prevent your passwords from being hacked by social engineering, brute force or dictionary attack method, and keep your online accounts safe.....

1. Do not use the same password, security question and answer for multiple important accounts.
2. Use a password that has at least 10 characters, use at least one number, one uppercase letter, one lowercase letter and one special symbol.
3. Do not use the names of your families, friends or pets in your passwords.
4. Do not use postcodes, house numbers, phone numbers, birthdates, ID card numbers, social security numbers, and so on in your passwords.
5. Do not use any dictionary word in your passwords.
6. Do not use two or more similar passwords which most of their characters are same, for example, ilovefreshflowersMac, ilovefreshflowersDropBox, since if one of these passwords is stolen, then it means that all of these passwords are stolen.
7. Do not log in to important accounts on the computers of others, or when connected to a public Wi-Fi hotspot.
8. It's recommended to change your passwords every 52 weeks.
9. Turn on 2-step authentication whenever possible.
10. Do not store your critical passwords in the cloud.
11. Access important websites(e.g. Paypal) from bookmarks directly, otherwise please check its domain name carefully, it's a good idea to check the popularity of a website to ensure that it's not a phishing site before entering your password.
12. Protect your computer with firewall and antivirus software, block all incoming connections and all unnecessary outgoing connections with the firewall.
13. Keep the operating systems(e.g. Windows 7, Windows 10, Mac OS X, iOS, Linux) and Web browsers(e.g. FireFox, Chrome, IE, Microsoft Edge) of your devices(e.g. Windows PC, Mac PC, iPhone, iPad, Android tablet) up-to-date by installing the latest security update.
14. If there are important files on your computer, and it can be accessed by others, check if there are hardware keyloggers (eg. Microsoft Word also has the ability to secure a word document with a password.
15. Lock your computer and mobile phone when you leave them.
16. Access important websites in private or incognito mode, or use one Web browser to access important websites, use another one to access other sites. I use three different browsers for different web sites.
17. Use at least 2 different email addresses, use the first one to receive emails from important sites and Apps, such as Paypal and Amazon, use the second one to receive emails from unimportant sites and Apps. You can a different email provider, such as Outlook and GMail to receive your password-reset email when the first one(e.g. Yahoo Mail) is hacked.
18. Do not click the link in an email or SMS message, do not reset your passwords by clicking them, except that you know these messages are not fake.
19. Do not tell your passwords to anybody in an email.
20. If an online shopping site only allows to make payment with credit cards, then check the web address and make sure it starts with "https" (or a padlock symbol that appears locked) as this will be a secure web page.

If you need more help with passwords, just ask our friendly tutors for help.

Alan Reeves

Family History Workshop

Family History Workshop held on the 28th September at 1:30pm

This will be a basic introduction to starting your family history and will include:

- How to get started
- Where you can look at records
- Different Sites for family History
- Different programs to record your family history online or on your computer.

Please book for this workshop as numbers are limited.

Mary McKernon

Scamwatch Updates

I know we are always mentioning this but I have been inundated with messages/SMS saying things like:

oc8ob You have a missed call. Caller left you a message: with a internet link. qbqb Telecom servibe provider has sent you a new notification: with an internet link, and various other misspelt messages suggesting that you "click" on the link provided.

No doubt this will open a web page that requests access to your device or asks for personal information etc. I also received a message from "Australian Post", not "Australia Post", which sent me to a very good imitation of Australia Post's website.

Coincidentally, I was waiting for a delivery at the time. Fortunately, when they asked for a few dollars to cover a redirection due to me not being home at time of delivery, I realised it was a scam. There does seem to be a huge influx of SCAMS at the moment.

By loading/using "Google Messages" You can "Mark as Spam" any SMS you received so any more you receive from that number will automatically be blocked and relegated to Spam Folder.

Also advising there is a free cut down version of Microsoft Office available at no cost but online, not a downloadable.

Click here for a link into ACCC's "Missed Call or Voicemail (Flubot) Scams".

Howard Andrews

Shopping Apps

It can be hard to keep up with what the supermarkets offer for online shopping, delivery etc. especially in these 'new' times of Co-vid.
I personally shop at my local supermarket which happens to be Woolworths so I am reviewing their services offered.

In the last lockdown I installed their App, made up a shopping list and used their direct to boot system to pick up my shopping. I found the system worked extremely well, there was an option to add requests like "ripest tomatoes possible please" and other choices regarding fruit and veg's. There is a minimum $30 order (which I believe applies to the Coles click and collect system).

I have not used their delivery services as I do not consider it worthwhile considering I do not order in bulk, I will certainly be using their direct to boot in future lockdowns.

If you would like help installing any of the supermarket apps or using their online services, book a lesson.
Here is a review on Woolworth's vs Coles online grocery ordering and shopping:
review-woolworths-vs-coles-online-grocery-ordering-and-delivery
Here is some information on Coles online shopping: **coles-online-updates**

Kathy Butler
