U3A BRIGHT UNIVERSITY OF THE THIRD AGE

EDITORIAL

SEPT 2021

By now I expect that everyone has been able to go on to our new membership system and update their details. U3A Bright holds personal information of our members and know the responsibility that this entails, so the decision was made to change over as the old paper based system was considered too insecure.

With many more people “going online” the decision was simple. The working party of myself, Marianne Dredge, Robyn Cirulis and Linda Hayes spent many, many hours of work getting the system up and running. All members information is now held in this sytem which is protected by a significant amount of security.

All of us must also play our part in this security by creating a secure password with which we access our details. I have included a couple of articles from the ACCC on scams in general and tips on how to create our own strong passwords.

If any member feels that they would like more assistance with the ‘online’ world, please reach out to your convenor or myself directly, I am only too happy to help in any way.

We are also looking at delivering short courses on digital technology. Tell us what you need.

Don’t forget…we have a new website……u3abright.org.au.

ACCC AUSTRALIAN COMPETITION & CONSUMER COMMISSION SCAMWATCH

Advice for older Australians

Scams target people of all ages and backgrounds, however, some scams are more likely to target older people.

Why older Australians are at risk

Often older Australians have more money and accumulated wealth than younger people, making them an attractive target for a scammer.

Scammers will also scour dating sites and social media for older Australians who have recently divorced or lost a long term partner, taking advantage of their inexperience with these sites and their often vulnerable emotional state.

Older Australians may also be seen by scammers as generally less internet and computer savvy or familiar with new technology.

Common scams targeting older Australians
Scammers take advantage of people looking for romantic partners, often via dating websites, apps or social media by pretending to be prospective companions. They play on emotional triggers to get you to provide money, gifts or personal details.
Investment scams involve promises of big payouts, quick money or guaranteed returns. Always be suspicious of any investment opportunities that promise a high return with little or no risk – if it seems too good to be true, it probably is – and is highly likely to be a scam.

This document is a publication of the Bright Branch of the University of the Third Age. 200 copies are distributed by email or at the Bright Library

Unexpected prize and lottery scams work by asking you to pay some sort of fee in order to claim your prize or winnings from a competition or lottery you never entered.
Inheritance scams offer you the false promise of an inheritance to trick you into parting with your money or sharing your bank or credit card details.
Rebate scams try to convince you that you are entitled to a rebate or reimbursement from the government, a bank or trusted organisation.
Door-to-door and home maintenance scams
Older Australians may also be more susceptible to door-to-door and home maintenance scams. While many legitimate businesses sell things door-to-door, scammers also use this approach. These types of scams generally involve promoting goods and services that are of poor quality, or not delivered at all.

Scammers may try and sell you gardening or roofing services, and then bill you for additional work that you did not agree to. Sometimes they may pretend to conduct a survey so they can get your personal details, or to disguise their sales pitch until they have been talking to you for a while.

Some of the warning signs you may be dealing with a scammer include:

- they visit late at night, or visit you again after you have said 'no'
- they don't show you any identification or give you any contact information, written quotes or receipts
- they might demand that you decide to accept their offer on the spot
- you may be asked for a deposit or full payment and can only pay by cash or credit card
- they fail to tell you about your legal rights, including rights to a cooling-off period.

Protect yourself

- Don't be pressured into making a decision. Scammers often try to create a sense of urgency through short deadlines, fake emergencies or threats of legal action.
- Be suspicious of requests for money – even if they sound or look official. Government departments will never contact you asking for money upfront in order to claim a rebate.
- Scammers will often ask you to use an unusual payment method, including preloaded debit cards, gift cards, iTunes cards or virtual currency such as Bitcoin.

- Verify the identity of the contact by calling the relevant organisation directly – find them through an independent source such as a phone book or online search. Do not use the contact details provided in the message sent to you.
- Don’t respond to phone calls or emails offering financial advice or opportunities – just hang up or delete the email.
- Always do your own research before you invest money and check the company or scheme is licensed on ASIC's ¸Money Smart Website.
- Be wary of people you meet social media or online dating sites who after just a few contacts profess strong feelings for you and try to move you away from the site and communicate via chat or email.
- Be suspicious of unexpected emails or letters advising you how to claim an inheritance or competition prize. Never give out your personal details and seek advice from an independent professional.
- Be aware of and understand your consumer rights.

- https://www.scamwatch.gov.au/get-help/advice-for-older-australians

PASSWORD TIPS

"Be sure to use a strong password" is advice we all constantly see online. Here's how to create a strong password—and, more importantly, how to actually remember it.

Using a password manager helps here, as it can create strong passwords and remember them for you. But, even if you use a password manager, you'll at least need to create and a remember a strong password for your password manager.

According to the traditional advice—which is still good—a strong password:

- Has 12 Characters, Minimum: You need to choose a password that's long enough. There's no minimum password length everyone agrees on, but you should generally go for passwords that are a minimum of 12 to 14 characters in length. A longer password would be even better.
- Includes Numbers, Symbols, Capital Letters, and Lower-Case Letters: Use a mix of different types of characters to make the password harder to crack.
- Isn't a Dictionary Word or Combination of Dictionary Words: Stay away from obvious dictionary words and combinations of dictionary words. Any word on its own is bad. Any combination of a few words, especially if they're obvious, is also bad. For example, "house" is a terrible password. "Red house" is also very bad.
- Doesn't Rely on Obvious Substitutions: Don't use common substitutions, either — for example, "H0use" isn't strong just because you've replaced an o with a 0. That's just obvious.
- Try to mix it up—for example, "BigHouse$123" fits many of the requirements here. It's 12 characters and includes upper-case letters, lower-case letters, a symbol, and some numbers. But it's fairly obvious—it's a dictionary phrase where each word is capitalized properly. There's only a single symbol, all the numbers are at the end, and they're in an easy order to guess.

Did you know your household could be eligible for

$250

off your power bill?

The Victorian State Government's Power Saving Bonus is a one-off payment to help eligible Victorians experiencing energy bill stress.

Available until 31st January 2022.

The $250 Power Saving Bonus for Pensioner Concession recipients and some Health Care Card holders (including JobSeeker, Youth Allowance, Austudy and Abstudy recipients) is now available. Before submitting an application for the bonus, please read the eligibility requirements.

Eligibility Requirements

- You must be a Victorian residential energy consumer (i.e. have a residential electricity account).
- You must be receiving payments under one of the following concession programs:
- Centrelink Pensioner Concession
- JobSeeker, Youth Allowance, Austudy or Abstudy
- Department of Veterans Affairs Pensioner Concession
- Or hold a Department of Veterans Affairs Gold Card
- Pension Concession Card holders who are not receiving payments, and Health Care Cards holders who are not receiving Youth Allowance, JobSeeker, Austudy or Abstudy payments, are not eligible.

Log on to: https://compare.energy.vic.gov.au/

then click the link to start your application

Submit a Power Saving Bonus application

This document is a publication of the Bright Branch of the University of the Third Age. 200 copies are distributed by email or at the Bright Library

great activities

President's Report

As I write this report the Victorian Premier announced a possible reduction in lockdown activities for regional areas except Shepparton. The need for us to be vigilant is obvious with the number of cases of Covid on the increase.

Prior to our normal August committee meeting, which we were able to hold at headquarters, the committee tried a zoom meeting. Congratulations to Helen who arranged the zoom meeting which was a success although we had a few problems...which we had anticipated. One of our members we could hear but not see, and another who had trouble staying online. However the experiment worked and Helen has run an inservice to improve our outcomes.

All Victorian U3A meetings are now being held in a zoom setting. Hopefully our restrictions will be lifted and we can reopen all our activities.

My quote for this newsletter is attributed to the Irish dramatist George Bernard Shaw (1856 - 1950)

"Life is not meant to be easy, my child, but take courage; it can be delightful."

Winter has been and gone leaving a lot of snow on the ranges. Spring has sprung so keep warm and enjoy what Spring brings.

Roy Ward. President

SCAMS AROUND

Wouldn't you know it?

Just when I included an article on scams in general from the ACCC and how to create strong passwords, I get several emails that are particularly 'dodgy'!

Easy to spot was the one from the Commonwealth Bank telling me that issues with my account would necessitate them putting a freeze on the account so I couldn't withdraw or deposit money unless I call on this phone number. As I NEVER click on ANY KIND of links in emails, of course I didn't call them.

BTW. I haven't banked with Commonwealth for over 50years!!!

Frightening to those who DO bank Commonwealth…… Be aware and go into the local branch if you are concerned.

The second one was NAB asking about a deceased estate and payment details. Yeah Well…….

The big scam going around at the moment and warrants a good warning to everyone is about the Vaccine Passports. They are offering them for a sum of money (of course!) even if you are NOT vaccinated.

Once you are fully vaccinated, go to the myGov website and get the DIGITAL CERTIFICATE.

This is an easy process when you have your myGov account. You just log in, click on Medicare and the certificate is available for download on to your computer and phone. I carry mine around on my phone.

Easy Peasy and no dollars out!

The Powers that Be haven't made any decisions on Vaccine Passports anyway!!!

COVID-19

The President of the Royal Australian College of General Practitioners, Dr Karen Price, says that "we must vaccinate as many people who are eligible as fast as we can".

All Australians over 16 years of age are now eligible to receive their 2 FREE doses of COVID 19 vaccine. Most people, young and older, who are currently hospitalised, in ICU or on ventilators with this disease are UNVACCINATED.

Being fully vaccinated is the clear path to your own good health & well-being and that of your family, friends and wider community. Think how wonderful it will be when we can again enjoy all the benefits of a COVID-safe normal life.

Unless you have a medical reason to not be vaccinated, please consider having the jab!

TO BOOK YOUR COVID VACCINE please logon to www.coronavirus.vic.gov.au select Vaccine then, book your vaccine appointment. Alternatively, you can call the booking hotline on 1800 675 398

Alpine Health has vaccine hubs at Bright Hospital (32-36 Cobden Street) on MONDAYS & Myrtleford Hospital multi-purpose room (30 O'Donnell Street) on TUESDAYS & FRIDAYS.

There is also the Wangaratta Vaccination Hub 53-61 Tone Rd, ph. 1800 571 121 which is open 9-4 MONDAY-FRIDAY.

Bright Pharmacy is offering injections one day per week. To book call 5750 1122.

What to take to your COVID-19 Vaccination appointment?

Valid I.D. e.g. driver's license

Medicare Card

Appointment confirmation email (if you have one)

You can also access a link to COVID rules and updates from our website u3abright.org.au on the home page or latest news tab.

This document is a publication of the Bright Branch of the University of the Third Age. 200 copies are distributed by email or at the Bright Library

Creating Strong Passwords

You'll need to create a password to do just about everything on the Web, from checking your email to online banking. And while it's simpler to use a short, easy-to-remember password, this can also pose serious risks to your online security. To protect yourself and your information, you'll want to use passwords that are long, strong, and difficult for someone else to guess while still keeping them relatively easy for you to remember.

Why do I need a strong password?

At this point, you may be wondering, why do I even need a strong password anyway? The truth is that even though most websites are secure, there's always a small chance someone may try to access or steal your information. This is commonly known as hacking. A strong password is one of the best ways to defend your accounts and private information from hackers.

Tips for creating strong passwords

A strong password is one that's easy for you to remember but difficult for others to guess. Let's take a look at some of the most important things to consider when creating a password.

- Never use personal information such as your name, birthday, user name, or email address. This type of information is often publicly available, which makes it easier for someone to guess your password.
- Use a longer password. Your password should be at least six characters long, although for extra security it should be even longer.
- Don't use the same password for each account. If someone discovers your password for one account, all of your other accounts will be vulnerable.
- Try to include numbers, symbols, and both uppercase and lowercase letters.
- Avoid using words that can be found in the dictionary. For example, swimming1 would be a weak password.
- Random passwords are the strongest. If you're having trouble creating one, you can use a password generator instead.

Common password mistakes

Some of the most commonly used passwords are based on family names, hobbies, or just a simple pattern. While these types of passwords are easy to
remember, they're also some of the least secure. Let's take a look at some of the most common password mistakes and how to fix them.

Password: brian12kate5

"I doubt anyone could guess my password! It's my kids' names and ages. Who else would know that?"

Problem: This password uses too much personal information, along with common words that could be found in the dictionary.

Solution: A stronger version of this password would use symbols, uppercase letters, and a more random order. And rather than using family names, we could combine a character from a movie with a type of food. For example, Chewbacca and pizza could become chEwbAccAp!ZZa.

Password: w3St!

"My password is so simple! It's just the beginning of my street address with a few extra characters."

Problem: At only five characters, this password is way too short. It also includes part of her address, which is publicly available information.

Solution: A stronger version of this password would be much longer, ideally more than 10 characters. We could also substitute a nearby street name instead of her current address. For example, Pemberly Ave could become p3MberLY%Av.

Password: 123abccba321

"My password follows a simple pattern, so it's easy to remember and type on my keyboard."

Problem: While patterns like this are easy to remember, they're also some of the first things a hacker might guess when attempting to access your account.

Solution: Remember that random passwords are much stronger than simple patterns. If you're having trouble creating a new password, try using a password generator instead. Here's an example of a generated password: #eV$plg&qf.

Password: BrAveZ!2

"I use the same passwords for all my accounts. This way, I only have to remember one password!"

Problem: There's nothing really wrong with this password, but remember that you should never use the same password with different accounts.

Solution: Create a unique password for each of your online accounts