SWITCHED ON SENIORS

Email : contact@computerpals.org.au

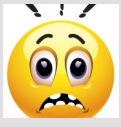
President

Sandra Keen

Dates to Remember

Friday, 26th May:
Tabpals @ 11am Apple
1pm Android
Friday, 2nd June
Next Enrolment/Open Morning 9:30—11:30 am

In This Issue



Australian Seniors Computer Clubs Association ASCCA

President's Report

Autumn and the cooler weather encourages us indoors earlier in the evening, giving us more time for projects such as learning a new skill. What better time than now to brush up on some computer skills. Some classes timetabled for this term are already full, while others have vacancies. To ensure your place in a class, book and pay early.

I have been asked why we don't have more classes, either later in the day or evening. The reason is clear when we consider that ALL our Tutors and people who work to make Computerpals Newcastle happen are Volunteers, giving their time freely to impart their knowledge so seniors feel more confident in this digital age. **National Volunteer Week** from **8th to 14th May** is held to acknowledge the generous contribution of Australia's Volunteers. So, because we couldn't do any of this without you, here is …….

May seems to be the month for Awareness because **National Consumer Fraud Week** will be held from **15th to 19th May.** The theme is **'scams through social media'.** With many seniors using Facebook and Twitter it is important to note that Scamwatch reports reveal that Australians lost over $9 million to scams of this type in 2016. Scammers take advantage of loneliness and the inability to do some jobs around the home. For more information see…

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

Also to be held from **15th to 19th May** is **Privacy Awareness Week** to raise awareness of privacy issues and advise us how to protect our personal information.

Finally, to all the **Mothers, Grandmothers and Great Grandmothers** in our club…. **Happy Mothers' Day** for **Sunday 14th May.**

Tech Talk

Advice for older Australians from Scamwatch

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.

Common scams targeting older Australians

Dating & romance

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 schemes

Investment schemes involve getting you or your business to part with money on the promise of a questionable financial opportunity.

Unexpected prize & lottery scams

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

These scams offer you the false promise of an inheritance to trick you into parting with money or sharing your bank or credit card details.

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:

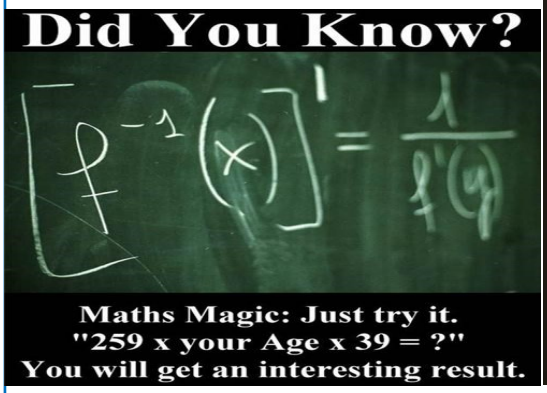
- they visit late at night, or visit you again after you have said 'no'
- they don't show you any identification or give you any contact information, written quotes or receipts they might demand that you decide to accept their offer on the spot
- you may be asked for a deposit or full payment and can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

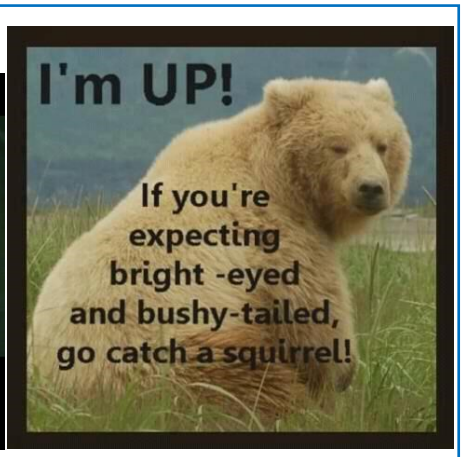
Protect yourself

- 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.
- 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 Moneysmart website.
- Be wary of people you meet on 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.

Funnybone—





While walking along the pavement in front of his church, our minister heard the intoning of a prayer that nearly made his collar wilt. Apparently, his 5-year-old son and his playmates had found a dead bird. Feeling that proper burial should be performed, they had secured it in a small box with cotton padding, then dug a hole and made ready for the disposal of the deceased.
The minister's son was chosen to say the appropriate prayers and with sonorous dignity intoned his version of what he thought his father always said: 'Glory be unto the Faaather, and unto the Sonnn, and into the hole he goooes.'

Keep that brain working; try to figure this one out....
See if you can figure out what these seven words all have in common?

1. Banana
2. Dresser
3. Grammar
4. Potato
5. Revive
6. Uneven
7. Assess

You'll find the answer at the bottom of page 6

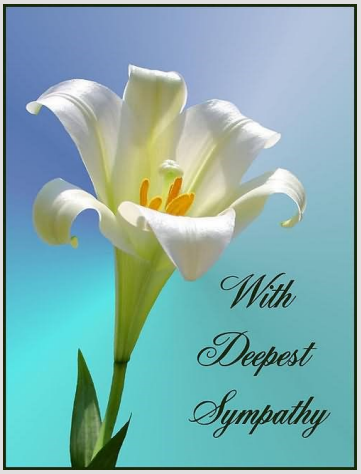

"There are better ways to log off."


A police officer called the station on his radio. "I have an interesting case here. An old lady shot her husband for stepping on the floor she just mopped."
"Have you arrested the woman?"
"Not yet. The floor's still wet."

Best Wishes

For all our members who are celebrating birthdays and anniversaries – hearty congratulations !

To those who are ill we send our best wishes for a speedy recovery.



Condolences

To those of our members who have lost loved ones recently, please accept our sincere condolences. You are in our thoughts.

Australian Seniors Computer Clubs Association ASCCA

Special Interest Groups

MemoryPals

*Our new group meets on **first Monday** of each month at **1:00pm** in the clubroom. Reminisce about your childhood memories and learn how to preserve them.*

WriterPals

*Our Creative Writing group is for enthusiasts, not experts. We meet on the **second Monday of each month** at 15 Hubbard Street, Islington. Meetings are **from 1:00 p.m.** until we go home!*

DigiPals

*DigiPals is an active group of ComputerPals members who meet on the **third Monday of each month** at **1 p.m.** in the Islington clubroom to explore digital photography.*

TabPals

If you have a portable device; iPad, Android tablet we have a Special Interest group called TabPals.
***The fourth Friday of the month** is our regular meeting **Apple devices** at **11 a.m**, **Android** at **1pm** in the **clubroom**.*

MemoryPals

The **next meeting** of this very industrious little group will be on the **5th June** at the clubroom beginning at 1pm.

At the May meeting our small group looked at suggestions on Pinterest for ways to display medals and plaques from sporting trophies, etc. We welcomed back Marilyn who brought along some old family photos and wondered how to prepare them for inclusion in a Photobook. Barry had fun photographing the old photos with his smartphone and restoring some of the images in Windows 10 Photos.

WriterPals

Greetings everyone. I hope your stories and poems for the ASCCA competition are going well. The competition closes on 4th September and that will be here before we know it.

Our next meeting is on **Monday 12th June** so please join us. We will be looking at some of our creative efforts and discussing some of the foibles of the English language and the tricks it plays on our ears and eyes and also the importance of punctuation and the differences one tiny dot can make to what we write. Placement of words and phrases can also cause some hilarity if used in the wrong place. Eg the piano that was bought by an elderly lady with carved legs

Give it a try—you might just surprise yourself.

DigiPals

Digipals group meets in the clubroom on the **3rd Monday** of the month at 1 pm. Next will be **Monday 15th May.**

The next Social Outing will be on **Saturday 3rd June.**

Watch your inbox for an email from Barry who will let you know *where the next get together is and other details.*

After the wonderful results in our own photographic competition for Seniors Week, we are VERY optimistic about the entries for the ASCCA competition this year. We are awarded points for every entry we send in for this competition, so give your photographic talents an outing and see what you can come up with. **Digital Photography** categories for 2017 are shown below. Each entrant could present one photograph, taken **after 10th August, 2016** for entry in each category - a total of seven entries.

1. Photo Journalism
2. Photo Travel
3. People/Portrait
4. Landscape/Seascape
5. Landscape, Structural/Manmade
6. Animal(s)
7. Open

More info and application forms will be made available when ASCCA publishes them

TabPals

This is proving to be a very popular group and many are finding it very helpful as a back-up to the actual classes where they can cement their knowledge and/or clear any queries they may have.
Next TabPals—**Friday, 26th May….**
Apple users—tablets and phones—meet at 11 am
Android users—tablets and phones—meet at 1pm
Bring your device fully charged.

ComputerPals Mission

Our mission is to educate seniors in the use of computers as a way of enriching their lives and making them more self-reliant.
We bridge the generation gap and assist seniors to find ways to benefit the community through their collective experience and knowledge.

Contact Us

To contact the Roster Team or the Treasurer regarding rosters or payments use:
islingtonpals@gmail.com

Roster Team

Barry Keen

Mitzi Gordon

Carmel Smith

Wendy Cripps-Clark

These people are all volunteers who also teach classes at Computerpals. We ask that you take this into consideration when your phone call is not answered immediately.

Beware of Google Docs phishing scam: Alert Priority High

Users are warned to be aware of a reported phishing scam involving a fake invitation to share a Google Docs document.

The scam sees a user receive a legitimate-looking email that may appear to be from a trusted contact inviting them to share a document on Google Docs.

Users who click on the link are directed to screens that request permission for a malicious service to access their email account, contacts and other sensitive information. If a user grants permission, the malicious service can impersonate the user when sending messages on to other Google email users.

Users may also face the risk of having information and messages from their email accounts compromised.

The scam reportedly targets Google personal and corporate email accounts.

A statement released on the Google Docs Twitter account said '*we have taken action to protect users against an email impersonating Google Docs, and have disabled offending accounts. We've removed the fake pages, pushed updates through Safe Browsing, and our abuse team is working to prevent this kind of spoofing from happening again.*
We encourage users to report phishing emails in Gmail.
If you think you clicked on a fraudulent email, visit g.co/SecurityCheckup and remove apps you don't recognise.'

Google Docs has also tweeted that they are '*working to prevent this kind of spoofing from happening again.*'

Spoofing occurs when emails are altered to appear to have come from a different source and is a method attackers commonly use to gain users' trust and increase the likelihood of a successful attack.

Staying safe
If you are unsure of the legitimacy of any message you receive, you should avoid clicking on any links or opening any attachments. You should check with the purported sender using contact details sourced from legitimate sources (not from the suspect message itself).
If you have clicked on the link or inadvertently granted permission to the malicious service, you should immediately revoke that permission using the steps recommended by Google Docs.

You should also check your account details to confirm that nothing has been changed and as an extra precaution, change your Google passwords immediately.

No matter how careful and savvy we think we are, we cannot rest on our laurels because the scammers are always working to separate us from our peace of mind and our money.

They call or email about car accidents, money owing to the tax department, friends stuck overseas and needing money to get out of trouble, your computer being blocked or infected with a virus, overdue accounts that will result in cancellation of services or bank accounts if not paid immediately. Their creativity in their lies is endless. They are nothing but parasites and need to be dealt with accordingly.

IGNORE THEM—THEY ARE SCAMMERS!

ComputerPals - Newcastle
Where Seniors master technology

Beware of fake myGov emails and SMS messages: Alert Priority High

You are advised that fake emails and SMS messages claiming to be from the Australian Government Department of Human Services' myGov website are targeting the community.
These fake messages seek to gather sensitive personal details from recipients and use them for malicious purposes.

Anyone who has received an SMS or email claiming to be from the Department of Human Services myGov and logged into their myGov account by accessing the link provided within, should contact the myGov helpdesk immediately on 13 23 07. People can also contact IDCare on 1300 432 273 for further advice and support.

The Department of Human Services does not include links in the SMS and email messages it sends to recipients. People should always log in by entering my.gov.au into their browser and check that https:// appears at the beginning of the address bar when you land on the site.

Fake myGov emails

The fake emails arrive with the subject line '*Australian Government and myGov must verify your identity*' and appear to be designed to capture users' myGov credentials and credit card information.
The links send recipients to fake forms that request the user input their myGov username and password and their credit card number, expiration date and security code.

These fake forms incorporate myGov branding and design and appear authentic. The emails appear to mirror fake myGov emails that were subject of an Alert from Stay Smart Online in February this year.
You are advised not to click on any links in these emails or submit any personal or financial details through any forms that these links may direct you to.

Fake myGov SMS

In addition, the Australian Communications and Media Authority (ACMA) has advised that a fake SMS claiming to be from myGov is in circulation.
The SMS campaign - apparently separate to the email campaign - aims to trick users into providing confidential personal identity information.
The fake SMS informs recipients in grammatically incorrect terminology that '*incorrect details*' are '*suspected*' in their accounts and demands that they upload correct documents.
The message then directs them to click on a link to a website that asks them to take a photo of documents such as passports or drivers' licences and upload these photos through the website.

Staying safe

You are advised not to click on any links in these emails or SMS messages, or submit any personal or financial details through any forms that these links may direct you to.
If you have supplied personal or financial information via this scam email or SMS, and any associated web pages and forms, immediately inform the organisations that provide services associated with your information.
These organisations may include your financial services providers (particularly banks); the Australian Passport Office; and the state government body responsible for drivers' licences in your state or territory. They will advise you of the next steps you should take to protect your information.

Stay Smart Online recommends you do not open emails from unknown senders and that you be wary of unexpected emails.
If you are unsure about whether an email is legitimate, contact the organisation, department or individual that it purports to come from, using a number you have independently located on a website, phonebook or bill, before opening the message.

Reporting cybercrimes

If your computer has been compromised, you can report the incident to the Australian Cybercrime Online Reporting Network (ACORN).

Answer to the word puzzle on page 3:
In all of the words listed, if you take the first letter, place it at the end of the word, and then spell the word backwards, it will be the same word.