



Winter Edition 2018

# Pennywise investments Newsletter

## In This Edition:

- ◆ Pennywise Update
- ◆ Review US!
- ◆ Infocus Conference
- ◆ Andrew Rieu Winners
- ◆ Nick Bruining  
"Book on Retirement"
- ◆ Article  
"The Art of the Password"
- Infocus Economic Update

## Review US!

Pennywise would love to hear feedback from all our satisfied clients.

Review Pennywise on  
Facebook

[Click Here to review Pennywise Investments >](#)



## Pennywise Update

### A word from Jeff

As we fast approach Christmas for the end of another year, I am sure it has been a hectic time for everyone. It certainly has been for us, with the fallout from the Royal Commission into the activities of the banks putting pressure on all the innocent parties to their practices. We have had a roller coaster ride on the share market in recent times with a potential Trade War between the USA and China being the main instigator. This will settle down at some stage but we have reviewed all client portfolios and re-adjusted portfolio's to have more cash at present, where appropriate to do so.

This will also present opportunities to buy in at a lower price at some stage in the new year.

The world will continue on in spite of all these things.

IOOF has been in the news for all the wrong reasons recently. This has not been as a result of issues with clients funds or that will directly impact clients, but a management issue and ASIC is also trying to show they are not the weak organization they have been in the past. The Gov't is wanting to put heads on the chopping block to try and show they are doing something. We have total confidence in IOOF to manage client funds and understand this can be a concern to clients but to please disregard some of the media reporting. If we had any doubts about IOOF at all we would withdraw clients funds and not be using them.

**Our office will be closed from Friday lunchtime on the 21<sup>st</sup> Dec and re open on Weds 2nd Jan 2019.**

Pina will be back in on Jan 2 and Jeff and Kerene back in the office from Mon Jan 14.

We would all like to wish everyone a very happy and safe Christmas and a healthy and good 2019. I thank you for your referrals to our business and the loyalty of so many clients with some having been with us in excess of 20 years.

A lovely feeling for us was being able to assist 3 generations from the same family which doesn't happen too often. It must be that we are getting older perhaps. It is very rewarding to have the trust of our clients and to know that we can make such a difference in people's lives by caring about their needs first.

Have a safe and lovely Christmas and we look forward to seeing you in the New Year.

**Jeff and The Pennywise Team**

**INFOCUS Economic Update (December 2018)** - [Click here to view the "Economic Update" >](#)

**infocus**  
Wealth Management



**Helping YOU Keep your  
PIGGYBANK Stocked  
During the Holidays**



Phone: (08) 9791 9113

Fax: (08) 9791 9114

Email: [pwi@pennywiseinvestments.com.au](mailto:pwi@pennywiseinvestments.com.au)

Website: [www.pennywiseinvestments.com.au](http://www.pennywiseinvestments.com.au)

"Like us on Facebook" [Pennywise Investments](#)

**DISCLAIMER:** PennyWise Investments makes no representation and gives no warranty as to the accuracy of the information in this document and accepts no liability for any errors, misprints or omission herein (whether negligent or otherwise). PennyWise Investments shall not be liable for any loss or damage whatsoever arising as a result of any person acting or refraining from acting in reliance on any information contained therein. The information contained in this newsletter is general information only. Kingsace Pty Ltd ABN 82 083 163 697 t/a PennyWise Investments is a Corporate Authorised Representative of Infocus Securities Australia Pty Ltd ABN 47 097 797 049 AFSL and Australian Credit Licence No. 236523 trading as **Infocus Financial Advice**.



## Infocus Conference

Kerene and I attended the Infocus National Conference at the end of October which was both very educational, daunting with some changes coming up and rewarding as well to mix with our peers.

### The Good News

Kerene won an award for her nomination as Team Member of the Year and was judged from all Infocus Offices Australia wide which is approx. 150 offices. Kerene has put a huge amount of work into making sure the back office runs as smoothly as possible. Well done to her.

### The Educational

We had a lot of very good speakers which were both work related and non work related. Steven Bradbury, Australia's first Winter Olympics Gold medallist was a key note

speaker and spoke of how he was perceived to be incredibly lucky to be the "Last Man Standing" and lucky to win his Gold medal. Hearing him talk of the 14 years of training, the serious injuries he had while competing, which could have cost his life and the fact he was unlucky when No 1 in the world to be one of those who was crashed into, to be eliminated when favourite, makes you realise how difficult the journey was. He was perhaps lucky on the day, but as he said, you still have to be there through qualifying and all the pre races and all the training for 14 years to get there. It was a will to succeed and shows no matter what, if we do the hard work, believe in the goal and give ourselves the opportunity, anything can happen. He was an excellent speaker.

### The Daunting

To be informed that all advisers who obtained their credentials prior to 2007 and even though working in our industry on a daily basis for 28 years, that our qualifications, experience and continuing professional development points will not be accepted and we have to go through a full university degree again of 8 subjects and approx. cost of \$3000 per subject to be re-educated was the most insane thing we could be told. But this is cold hard fact.

To also be told we will have to sit an annual exam of approx. 3 ½ hrs that is not even related to the work we actually do was also unfathomable but will be compulsory no matter what we think. Again, at a considerable cost to advisers.



## Andre Rieu

On Sat Nov 24 we attended at Perth with the lucky winners of our referral and adviser ratings raffle draw which was run from the previous 12 months. All clients were given a ticket in the draw who either referred someone to the business or gave us a rating on adviser ratings.

The lucky people drawn and we had a lovely evening with was Brian and Rhonda Zanich, Eric and Joyce Wootton and Dan and Linda Luttrell

who bought their tickets but came with us. It was a great concert and he is a great entertainer with his entourage.



## Nick Bruining Book on Retirement

A couple of people have said they got the book, which is great to be educated. I do not agree with him at all on the basis that you only need \$250 000 to have a carefree wonderful retirement and what you get from Centrelink fills the gaps.

I have a big issue with relying on Centrelink for a start, as the rules keep changing and if you rely on this as your main future source of income, then you may be severely disappointed. This isn't directed at those on a pension now, but especially those in the future.

Next thing he says is that \$250 000 will give a comfortable income of \$48000 pa. Definitely, there are those who do live on \$48 000 or less, but on average most couples retiring now

would struggle to live on anywhere near \$48 000. It is not going to provide a comfortable retirement.

Another point it misses is what happens when you have to replace cars, have larger home repair costs, or larger holidays. That will drop your capital and then if you live longer than expected are at far greater risk of running out of money.

I encourage all people to try and save so you have a retirement that is closer to what your pre retirement net income is so you can enjoy holidays, do the things you enjoy and not have to stress so much. I think his picture doesn't paint the real story. Be educated but also be aware of relying on those types of wishful thinking for the balance of your retirement years, depending always on what stage of life you are at.





# The Art of the Password

Sourced from "Midwinter"

## Top tips for password management

When it comes to cyber security, the password is the topic de jour. Everyone knows that a password is the most common mechanism to provide authentication. Positively, unlike facial and fingerprint recognition, passwords can be changed.

However, the problem with "the password" is through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember but easy for computers to guess.

In the old days, the quality of a password used to be linked to its length (entropy) – for example – 'correcthorsebatterystaple'. But now the *uniqueness* of a password is considered an essential element when choosing a password, and conversely *predictability* is a key part of cracking them.

In other words, you want to make your password as unpredictable as possible. This means if you can pronounce your password, or if it includes words that commonly go together, it's not a password and it's easy to crack.

You may think your password is creative and difficult but it would actually surprise you just how common the same words, tricks and combinations you use are.

Here are the 50 most used passwords. You will want to make sure your passwords aren't on this list as a basic minimum!

### The 50 Most Used Passwords

- |              |              |                |
|--------------|--------------|----------------|
| 1. 123456    | 11. 123123   | 21. mustang    |
| 2. password  | 12. baseball | 22. 666666     |
| 3. 12345678  | 13. abc123   | 23. qwertyuiop |
| 4. qwerty    | 14. football | 24. 123321     |
| 5. 123456789 | 15. monkey   | 25. 1234...890 |
| 6. 12345     | 16. letmein  | 26. p*s*y      |
| 7. 1234      | 17. shadow   | 27. superman   |
| 8. 111111    | 18. master   | 28. 270        |
| 9. 1234567   | 19. 696969   | 29. 654321     |
| 10. dragon   | 20. michael  | 30. 1qaz2wsx   |
| 31. 7777777  | 41. harley   |                |
| 32. f*cky*u  | 42. zxcvbnm  |                |
| 33. qazwsx   | 43. asdfgh   |                |
| 34. jordan   | 44. buster   |                |
| 35. jennifer | 45. andrew   |                |
| 36. 123qwe   | 46. batman   |                |
| 37. 121212   | 47. soccer   |                |
| 38. killer   | 48. tiger    |                |
| 39. trustno1 | 49. charlie  |                |
| 40. hunter   | 50. robert   |                |

Aside from picking common words, there are other red flags that may not be as obvious when it comes to picking a password.

## We recommend, as a general guide:

1. DO NOT use one password across various applications – this means if a hacker manages to hack even just one application where you have used this password, they will now be able to access your login across all of the applications where you have used this password. Often this can mean access to private, personal, professional, financial and medical data. Alarm bells anyone?
2. DO NOT change your password routinely or enforce your staff to change their password routinely i.e. every 90 days etc. This used to be seen as a good idea – with the logic behind it being that if a password were stolen, then it would lose its value when the user goes to change it. In reality however, individuals end up just rehashing similar versions of their password over and over again, or even worse – just keep forgetting the latest iteration and then continually need to reset. It's a nightmare.
3. DO NOT use a password that is an actual word – if you can pronounce your password, it's not a password and it will be cracked. If you want to use real words rather than a jumble of characters, use a combination of words that have no relevance or connection to each other for example – aladdinlattetissuelipstick

**If you want to take some simple and easy steps when it comes to password management, make sure you ARE doing the following:**

1. DO use a password manager – for example LastPass. This way you can store all of your passwords in one place without the need of remembering all of them. You only need to remember one password – that's your LastPass password.
2. DO use a strong password generator (you can find a range of them on google) to help you generate different difficult passwords for all your applications and then store them in LastPass.
3. DO use applications which encrypt your passwords. This means if you forget your password, the application should not be able to tell you what it is, because they aren't storing them in their base form.

