

Club Room

ARV Computer Club
Member Resources
First Aid Service



This is a checklist to help avoid scammers causing you problems.

Prepare to avoid scams

There are many types of scam but you can prepare yourself so that you are ready for any scam attempts. Try to do as many things as possible on this checklist that will be helpful for you if you get scam messages or calls.

Action	Check
Gather phone numbers in advance for critical accounts like banking so that you know the correct number to ring if you are worried about a possible scam message.	
Set up two-factor access to critical accounts like banking. This means that if your password is stolen criminals cannot get access to your money without a second piece of information like a phone code.	
Use a different password for every account so that the loss of one password does not compromise everything.	
Read Scamwatch for current information about scams so you are aware of what is possible. https://www.scamwatch.gov.au	
Check the advice from Computer Club in Friday Night Update and Bits & Bytes	
In case a scammer tries to impersonate a family member in trouble, arrange a secret word or phrase with family members in advance so you really know who it is. Never mention any family names until you really know it is a family member talking or texting.	
Practice answering the phone with 'Hello' only and wait for a response to make it difficult for scammers to record your voice to fool your family.	
Practice answering calls only from numbers you know and ignore the rest	
Minimise disclosure of personal information on social media to minimise scammer information sources	
Check your email is not known by criminals at https://haveibeenpwned.com/	
Check your password for security at https://haveibeenpwned.com/Passwords	
Keep the Computer Club number handy for our advice 8853 1810, but do not respond to suspected scam messages	