An older persons guide to protecting our digital stuff

The elderly and retired have been forced into the use of digital devices.

It maybe to talk to the children and grand children, look at family photos and videos, it maybe to access government services and/or to access banks, credit unions or super sites.

In most cases you have had to take that leap and invest in a smart device, computer or a tablet.

The cybercriminal is waiting for you to make a mistake.

No one wants to be a target of a cybercriminal.

No one wants to be scammed, to be taken for a ride.

Here are some ideas that will make you less of a target.

Ideas to stop you being a victim of cybercrime!

Passwords. Pass phrases and pass codes:

Passwords, pass phases and pass codes are your passport to the digital world. Protect them as such. You device needs a pass core do not leave it so that any one else can access your device. Your sites and services need a password or pass phrase. All passwords and pass phrases need to be unique for every different site, they have to have complexity (numbers, letters, capitals and symbols) and they have to be longer than 10 characters. Passwords need to be like this because we need to stop computers hacking them. They should not contain any personal information.

Get a password manager:

Remembering all those passwords and pass phrases is a nightmare. The best solution is not to write them down (physical or digital) but to get a password manager. It stores them where you can access them easily but is super secure because only you can access them.

Use a third level of security:

Passwords and pass phrases can be stolen. They can be stolen because you have done something wrong, a site you belong to has been hacked or because you were using an easy password like **qwerty** and a computer broke it. We need a third level of access (2 factor/multi factor authentication) to augment who you are (username) and what you know (password). That third level is what you have. An SMS to your phone with a 6 digit code or use a application on your phone that produces a 6 digit code. **NEVER GIVE THE CODE AWAY TO ANYONE NO MATTER WHAT**.

Trust no one:

The internet is full of unsavoury people all trying to steal stuff from you. They also know that your are a trusting person because you are a baby boomer and your upbringing makes you a more trusting person. Even your kids, grandkids can trick you into making a mistake. The worst type of betrayal is thinking that that email, sms or phone call is from a loved one when it has come from a scammer looking like them. Always “verify then trust”. If you are not sure call them on the phone (the number you have for them not the one that you think is from them).

Don’t panic:

The cybercriminal relies on scaring you using what I call FUD (fear, uncertainty and doubt). Nothing that you are doing in the digital world is time sensitive, is going to get you arrested or have someone come round to you house. No business especially a government department or large organisation will accept gift cards or money transfers as legal tender. If they want to be paid in this way they are scamming you.

If it is too good to be true its too good to be true:

No one is going to deposit a million dollars into your bank account—EVER, especially it they require you to spend 10K to do it. The scammers rely on hooking you with barely believable scams based on things that are just a little bit to good to be true. If they tie in a sense of urgency then they get more people.

CARE MANAGED IT

CareMIT Pty Ltd. Unit 3, 116—118 Wollongong Street, Fyshwick, ACT 2609. Phone:- 0262577792 Email:-directors@caremit.com.au

Social media is not your friend:

The social media platforms, although they are a great way to communicate and have a little fun, are there to sell you stuff. We use the phrase "if it is free then you are the product". Do not put too much personal information on social media platforms, be aware that the algorithm feeds your likes because they want to keep you on their platform. Always implement the tightest security around you account.

Be prepared to say NO:

There is no one holding a gun to your head. Saying NO as a first response to anything and everything on the internet is good digital hygiene. Say NO more often.

Log out where possible:

All devices have a timer that locks the screen. Use it. Always shut down or lock your smart devices so no one else can access it when you are not around. On computers each user should have a separate account and that account requires a password.

Check all security settings regularly:

Social media, sites and service on the internet need to have their security sessions checked to ensure that they have not been reduced. Checking them regularly also ensures that you are moving more sites to multi factor authentication.

Back up your stuff:

There is loads of personal information on our devices. Information that is only available on that device. You need to back it up. Always use the 3,2,1 plan. Three copies of all data in 2 different locations and one location has to be off site and disconnected. We have a great off site secure backup solution for seniors. One drive and google docs need to also be backed up.

If it tells you to update—DO IT!

Updates and security patches are a regular occurrence in todays world. They are an important part of being secure. Always do updates in a timely manner.

Use technology to stop the criminals:

Technology is a great leveller but not the only one. All devices have a firewall—USE IT. Protect your device (including apples) with an anti virus product (end point protection) - preferably not a free one.

Get some professional help (no your 11 year old granddaughter is NOT help):

Using your grand daughter to help you on a computer is a great way to bond. It is not, however, the best way to get help and support for your device.

Do some additional awareness training:

If you want to be more aware of what the cyber criminal is capable of you need to get some awareness training. There are free awareness training platforms all over the internet but we do recommend https://wizer-training,com.

Have you thought about what happens when you are gone:

Not being macabre here but if something happen to you, you need to have a contingency plan. My recommendation is to put a codicil in your will and nominate someone to clean up your digital foot print. Put your username and password of you password manager in your will.

Upgrade regularly:

Digital devices are not power tools. They have a recommended "shelf life" before they become obsolete and obsolescent. The older they are, if you are using them the more vulnerable they become

Find out where you could improve:

Think you are secure? Here is a simple way to see if you have forgotten something. Go here https://retire.scoreapp.com and complete the 24 question, read your report and make your decision