

> PC Update

September 2022



From The Editor September 2022	2
Foxtel Cancellation, Network Switch Failure and Lifetime Warranty ..	3
My First Encounter With Linux	11
The Tesla Optimus robot is not very impressive – but it may be a sign of better things to come	14
What is multi-factor authentication	16
DOTW Highlights	18
East SIG Report August 2022	19

From The Editor September 2022

Hugh Macdonald

Hello and welcome to another edition of PC Update.

This month we have a couple of interesting articles from members. There's one from Steve on his experiences of cancelling Foxtel and on the way discovering that his network switch had also failed, and dealing with the lifetime warranty on the device. In this age of 'cord cutting' it's an interesting article from that point of view, and whether consumer guarantees really do hold up.

Stewart Gruneklee has also written of his first steps in using Linux. There's a lot of interest around Linux from readers of PC Update, and with the decision by Microsoft to drop support for a lot of fairly recent computer with Windows 11, Linux is becoming more and more of an option. So Stewart's take on it is a good read.

There's also some articles on multi factor authentication, robotics and some of the usual columns like the East SIG Report, DOTW, and Interesting Internet Finds.

Foxtel Cancellation, Network Switch Failure and Lifetime Warranty

Steve Stubberfield

This is my story about how cancelling our Foxtel subscription lead to a network switch failure and what is meant by life time warranty.

It all started when we decided to re-assess what subscription services we required. With so many different services now requiring monthly subscriptions it is almost impossible for the average person or family to afford all of them. So we sat down and discussed what we really needed, or more to the point, wanted. High on my wife's priority list is watching tennis, while for me it is watching Sci-Fi or action movies or series.

For many years we have had Foxtel with an IQ2 box and a legacy package which included the sports pack at \$96 per month. Last year Foxtel discontinued the On Demand feature for the IQ2 and more recently have advised that the IQ2 box would be phased out and cease to function, so this added a little more urgency to our decision. While we could have upgraded our Foxtel package (they did offer a better deal), we knew it wasn't good value for us because there was hardly anything else we were watching on it other than the tennis and I also wasn't keen on getting a satellite dish installed on the roof either. We have also had Netflix for several years and, more recently, my sister pays part of the subscription to upgrade to premium.

The decision we made was to cancel Foxtel and, with the money saved from that, sign up to various other services, starting with Kayo and Stan, and then to look at adding others like Binge, Disney and Amazon Prime. Even with all of those, we will be slightly better off. So, in January we signed up for Stan (for the Aus Open) and then in February we signed up for Kayo and cancelled Foxtel. Of course there's always the option to start or stop these services any time as required and we may not add them all immediately. In fact we added on Stan Sport just for January which is \$10 extra and we will do it again three more times in the year for the other Grand Slam tournaments. We also have the option to log in to Foxtel Go using my Dad's account if there was something in particular that we really wanted to see on Foxtel. At the time of writing, my calculations were as follows:

Existing: Foxtel + Netflix

$\$96 + \$17 = \$113$ per month

New: Netflix + Stan + Stan Sport* + Binge + Kayo + Disney + Amazon

$\$17 + \$14 + \$3.33 + \$14 + \$25 + \$12 + \$7 = \92.33

(*Stan Sport is calculated as \$10 per month x 4 months, as mentioned above. This averages to \$2.33 per month over the year. Note also that prices for some services are priced at just under the dollar, like \$16.99, and these have been rounded up to the nearest dollar for simplicity).

So that's a saving of over \$20 per month and, in my opinion, the viewing choices gained, outweighs the choices lost from Foxtel. There are also additional discounts to be had over the first year, such as \$7.50/m for Kayo and \$2.33/m for Binge if you have a Herald Sun digital subscription, and \$2/m for Disney and \$2.08/m for Amazon if you pay yearly. This adds up to an additional saving of almost \$14/m for the 1st year.

No doubt these changes will increase the load on our internet connection. With four users in the

household using the internet, we had noticed our usage slowly trending upwards over the years. Our son moved out of home last year, thereby reducing the usage, but this has been offset by the increase in HD and 4K content, so the upward trend has continued. We currently have a 100Mbps 500GB plan and, for the first time, we received an 80% usage warning in January (mainly due to the Aus Open). However, if required, we can easily make that unlimited for an additional \$4 per month and still be in front.

So the next step was to remove the IQ2 box. This was the first step leading up to the switch failure. To put you in the picture, we have a primary (premium?) viewing location, the Rumpus room (See Photo 1), and a secondary viewing location, the Lounge room (See Photo 2). Both locations have a low-line entertainment cabinet, a Samsung Smart TV, a Blu-ray player and an AV Receiver. The Rumpus room also has a CD player, an old Topfield Hard Drive Recorder and a more recent Beyonwiz recorder, whereas the Lounge room also had the Foxtel box and a Wii game console. Our home network consists of a network cabinet under the stairs containing a 24 port patch panel, a Hewlett Packard Procurve 1810G-24 network switch, an Arris NBN cable modem, a Billion 7800VDPX router, a Synology DS413 NAS, a video distribution module and various plug packs and power boards. The house is wired with Cat6 cable which connects all the 'permanent' devices while all the portable devices connect via WiFi. Just as an aside, I have a new Synology DS920 NAS and I'm in the process of changing over from old to new.

After removing the Foxtel box, we decided to relocate the old Topfield HDR to the Lounge to fill the void in the cabinet. The lounge only has two network ports and we originally needed four devices connected so I had placed an old ADSL 1 modem/router under the cabinet and configured it in bridge mode to use as a switch. Since the Blu-ray player is rather old and is no longer upgradeable, there's no need for it to be connected anymore and with the Foxtel box gone, the ports needed came down to two but then went up again to three by adding in the Topfield HDR. We decided the Wii console could remain disconnected and be swapped over with the HDR when we needed it. This allowed the router, plug pack, power board and several cables to be removed, thereby removing some of the clutter under the cabinet.

After removing the Topfield box from the Rumpus room there was some reconfiguring required there too, as well as some overdue dust removal! This then lead to some further changes in the network cabinet and I thought, while I was at it, I might as well tackle another change I had in mind for some time regarding the power to the cabinet. There was also the previously mentioned new NAS to accommodate.

The network cabinet is a rather typical 12RU metal cabinet with a Perspex front door (See photo 3). It has no holes in it other than ventilation slots and a large opening in the back panel. It is mounted on an internal plaster wall in a cupboard under the stairs and there is a large cut-out in the plaster to match the cabinet back panel. All the cables - network, video, antenna, Foxtel - come to this point from under the floor or through the ceiling space. See photos 4 & 5 for before and after views of the bottom.

When the cabinet was installed there was a problem with getting power into it. About half a meter above the cabinet there is a double power point but I didn't want to have a lead dangling down over the front of the cabinet which would prevent the door from being closed and I didn't want to drill a large hole in the cabinet for a power lead. My solution was to drill a very small hole in the plaster immediately above the cabinet just out of eye sight and just big enough for a power lead (not the plug). I then placed a four gang switched power board in the cabinet, cut off the three pin plug, fed the lead up the wall cavity and through the small hole, fitted a new three pin plug and plugged it into the power point. I was never entirely happy with this arrangement because it was not easily changed and I had to have additional power boards plugged into the first one because of plug packs being too wide and blocking the point next to it.

I realised recently that I had a spare low profile power point that would fit neatly on the back panel of the cabinet between the opening and the top panel. So I hatched a plan to remove the power boards, drill holes in the back of the cabinet and through the plaster to accommodate the switch and then connect the switch to the power point above. Due to a noggling in the wall cavity, space was tight so drilling accurately was critical with only a millimetre to spare either side. This also involved a specially shaped block of

timber with pre-drilled holes that needed to be manipulated into the wall cavity above the nogging to accommodate the power point screws because there was no way of using a traditional power point plaster mounting bracket. I ended up creating a 3D model using Sketchup and printed out a drilling template. See photo 6 for the new power point.

Part of the plan was to install a new multi-gang power board and I wanted to mount it to the rack so that it was out of the way. There are numerous models designed for this purpose but they are all rather expensive. I eventually found a six gang non-rack type for only \$8 at K-Mart and it had three wide spacings to accommodate plug packs. In order to mount it to the rack, I first mounted it to a piece of timber and then mounted the timber to the rack. I could have used aluminium but that was more difficult. See photo 7.

In order to carry out the modifications, I needed to power down, disconnect and remove all the devices and also lower the patch panel out of the way. I then used the template to mark out the holes and began drilling. Next I had to manipulate the specially shaped backing block into place in the wall cavity. I can't even begin to describe how tricky that was but it worked perfectly in the end. Once completed, I began to put everything back together and after reinstalling the network switch, I powered it up. That was when everything ground to a halt.

The network switch fault light illuminated and was associated with a high pitched whine and it failed to boot up. My guess was that the power supply had a problem. My first thoughts were what I could do to get some things working. I had three spare ports on the Billion Router, so I patched in my PC, my wife's PC and the NAS. I then realised that I could also daisy chain the aforementioned ADSL 1 Router to gain another two ports and get the printer connected. The Billion Router is also the WiFi hotspot so all the portable devices were ok and I was able to change over the security cameras and TV's to Wi-Fi. Everything else had to wait.

The next issue was to fix or replace the network switch. I did think about opening it up, thinking it would most likely be a blown capacitor but I didn't want to do that because the unit supposedly had a lifetime warranty. So I jumped on the HP web site and entered the serial number for a warranty check but it didn't find it, however the model was specifically listed as having a lifetime warranty. Hewlett Packard has apparently split into HP for consumer products and HPE for enterprise level devices. My device is apparently classified as an enterprise level device. I had trouble finding what to do for servicing on the HPE website because it was geared towards businesses that would already have their products registered, which I didn't. I noticed that the site language was set to US English and didn't think much of it. On a whim I clicked on the list and it had an option for Australian English, so I selected it, and then an Australian oriented page appeared with an Australian contact number. I didn't expect that, English is English, right?

So I called the number which was automated with specific options and voice recognition. All I had to do was say "network switch", and then "Procurve", and then the call was transferred and a woman with an American accent answered (in California). I told her my problem and she took my details but then she said that my email address was not a company address. I told her that I was not a company but I have the original purchase receipt from July 2012 (yes, just short of ten years ago!). So she sent me an email and asked me to reply with a copy of the receipt and she waited while I did so. She then had to check with a supervisor and then told me they would progress my case and hand me over to someone else to go through the fault details. The second person asked me for more details about what happened leading up to the problem and then told me she would progress my case further and the call came to an end.

About half an hour later I got an email requesting a photograph of the unit showing its serial number, which I also complied with. About an hour and a half later I received another email stating that my case would be proceeding. Then twenty minutes later another email stating a replacement "part" was being sent, the "part" being a complete unit. Another email followed with tracking information and instructions. Three days later the part was on my doorstep! That was exceptionally good, considering it came from

Homebush in the middle of the floods. The package had instructions to put the old unit in the same packaging as the replacement unit, put on an address label that they provided and let them know when it was ready for collection. They then arranged for a courier to come and collect it. Three days later the old part was gone!

There was a slight hiccup with installation because I couldn't find a saved config file which meant I had to do it all again manually. Since it's a semi managed switch, it's not plug and play, so it has to be plugged directly into a PC to be configured initially. Anyway, it's now installed and configured and my network is back to normal. I should point out that the replacement unit was a refurbished one since that model is not in production any more, but I think that's perfectly reasonable. I have no idea why it failed, but this was the first time since it was installed that the power cord was removed and there seemed to be a bit of movement of the power socket on the case. Maybe that physically disturbed something. By the way, in case you're wondering about wiring the power point, one of my mates is licensed to carry out electrical work.

So there you have it. I hope you found this interesting. Perhaps it is time to do your own review of streaming services. And if you have a HP network switch with a lifetime warranty, make sure you keep that receipt!



Photo 1: The Rumpus room setup with 75" TV.



Photo 2: The Lounge room setup with 65" TV.



Photo 3: The whole cabinet. Note the small hole in the plaster above where the old power cable emerged.

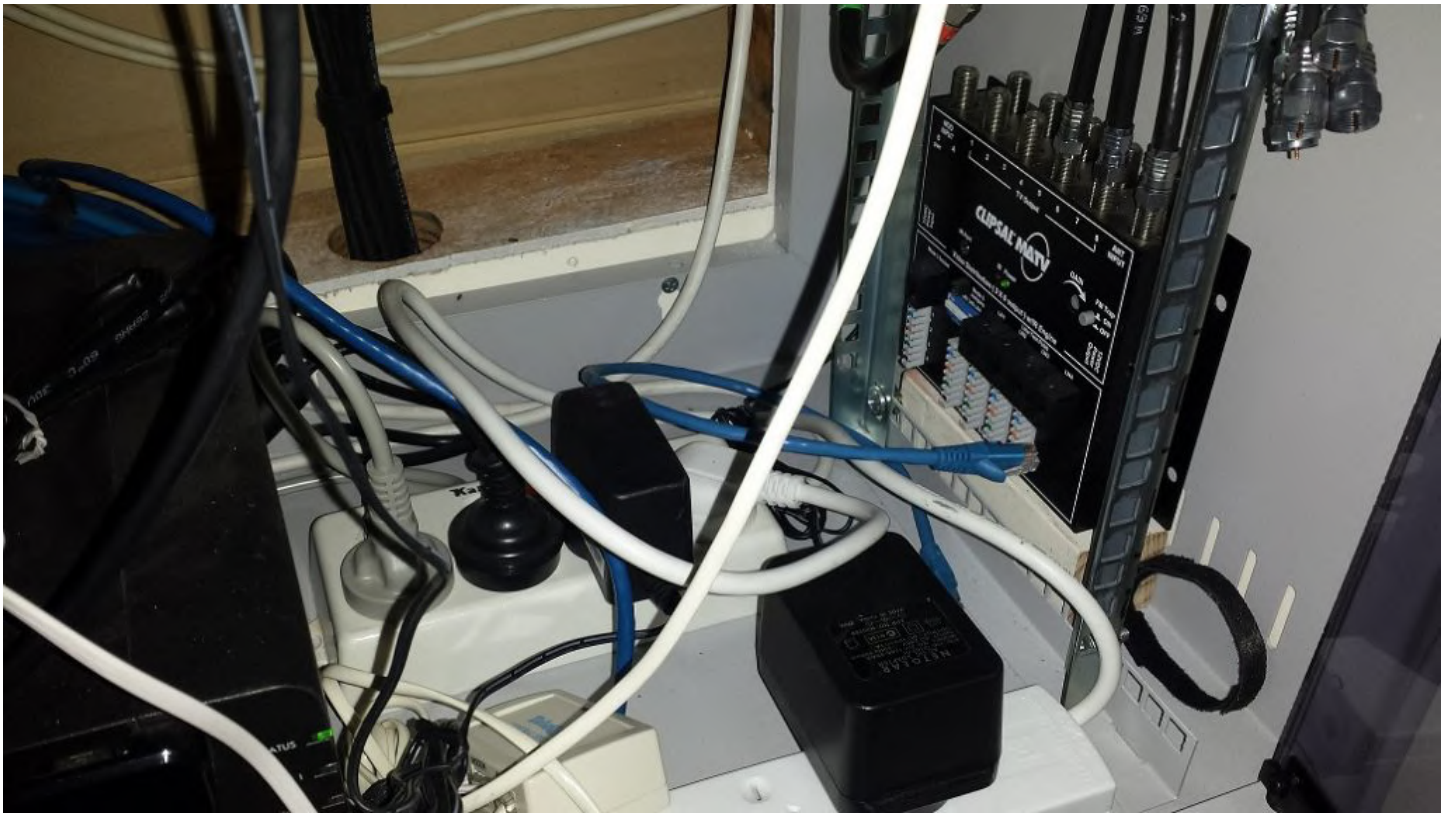


Photo 4: Bottom of cabinet showing the old power boards. You can also see the video distribution unit.



Photo 5: Bottom of cabinet with the old power boards removed, thereby freeing up some space. You can see the Synology NAS on the left with the Billion Router on top and the Arris NBN modem to the right.

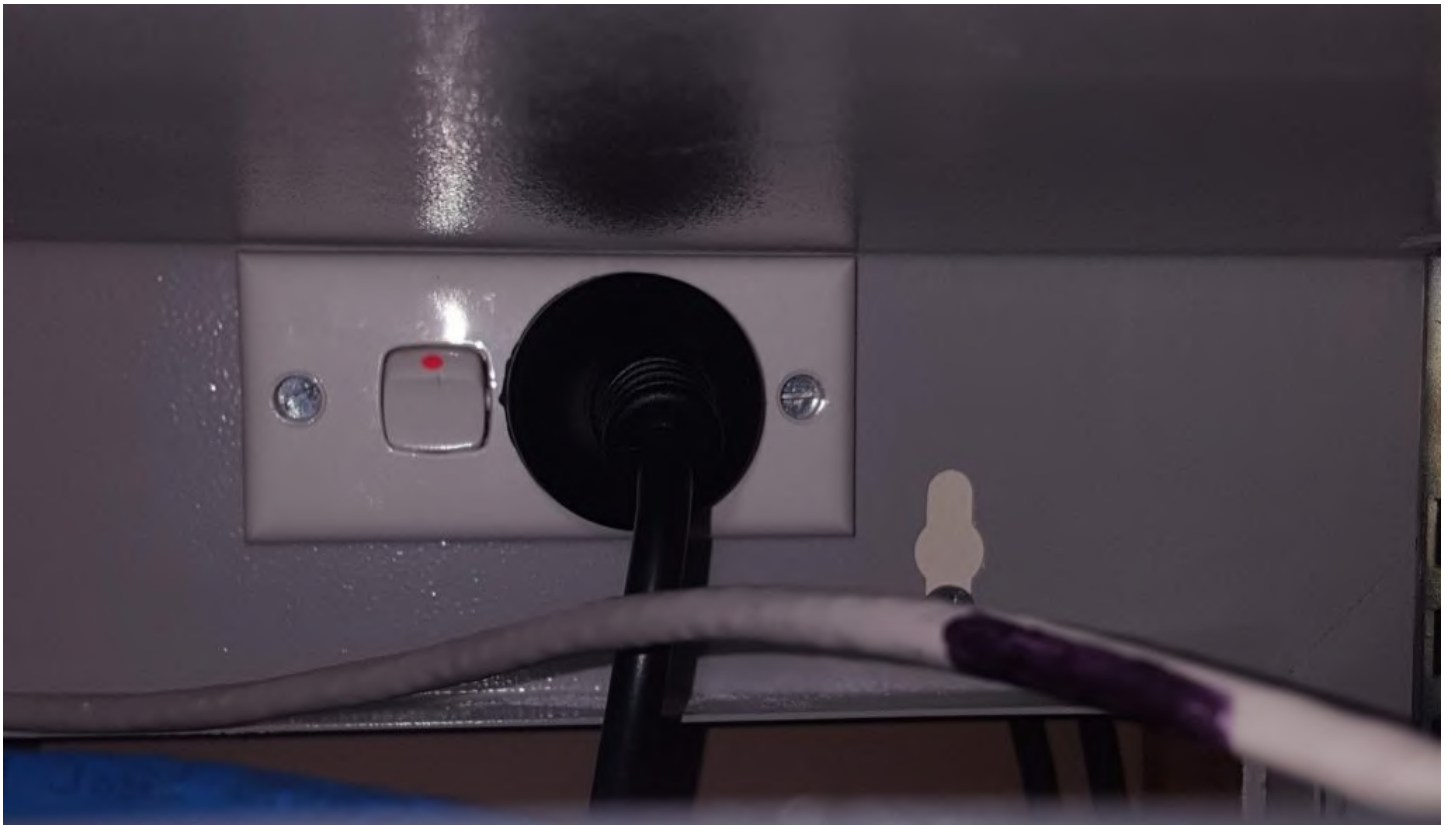


Photo 6: The new slim line power point installed on the back panel. There is a nogging behind it that covers from the bottom lip of the panel to just below the switch mechanism, hence the need for accuracy.



Photo 7: The new power board mounted on a piece of timber. Despite the wider spacing for plug packs on the right, due to the stupid design of one of them it still doesn't fit there and had to go on the far left.

My First Encounter With Linux

Stewart Gruneklee

The personal computer operating systems that I have used over the years started with Digital Research DR DOS in the mid 1980's and then Microsoft's DOS followed by various versions of Windows starting from version 3.11 up to the current Windows 10. Microsoft loudly proclaimed that Windows 10 would be the 'last' version of Windows and would be regularly updated ad infinitum. Well, that policy got thrown out with the introduction of Windows 11 and the major change being that anything other than relatively recent computers would simply be unable to run the new system. As always there will be some computer users that will work around such limitations and run Windows 11 on older computers, but at the risk of not getting updates or support from Microsoft.

Unix and then Linux were operating systems that I had heard of but had paid little attention to because the company I worked with (prior to retiring) was locked into Microsoft and it was convenient for me to use the same systems and software at home as well as at work. The introduction of Windows 11, however, changed my mindset. For a start, my seven year old ASUS laptop computer is in perfect working order and I have recently replaced the 250GB Solid State Drive (SSD) with a brand new 500GB SSD. A new equivalent computer replacement that will accept Windows 11 would cost me about \$1,500 for very little gain in performance or utility over what I already own.



This PC doesn't currently meet
the minimum system
requirements to run
Windows 11

So what should I do? Windows 10 is supported by Microsoft until mid-October 2025 (unless there is a policy change in the interim. By that time my laptop will be ten years old, but if still in good working order, why discard it? With the encouragement of other Melb PC members, I decided that I would explore the possibilities of cutting my ties with Microsoft entirely and trying out Linux as an alternative operating system. I have already dumped the Microsoft Office applications several years ago and embraced the open source Libre Office and Thunderbird as replacements and never want to go back to the Microsoft offerings, as good as they are.

By nature, I am cautious of 'burning bridges' so the plan was to find a spare computer to do my Linux exploring. I remembered that my first laptop computer, an ACER Travelmate 8472, Intel i5 CPU with 8GB RAM, was still hiding in a cupboard. This ACER laptop was originally purchased in 2011 running Windows 7 Pro and it was replaced with a much nicer ASUS laptop machine in 2015, which remains my normal workhorse. This older ACER laptop has been sitting in a cupboard for the past seven years and needed the battery to be charged up before it would respond. The battery is still rather frail and therefore the computer needs to be constantly plugged into power when in use.

The next job was to remove the Hard Disk Drive (HDD) and replace it with a spare 250GB SSD to gain some speed of operation. The plan then was to load Linux. The question is which Linux? I have little experience of Linux and this is precisely why I want to do it. I note that Ubuntu is being used in the computers in the Lounge at Moorabbin and my first thought was to do likewise because they seem easy to use. I have kept a copy of the PC Update article by Hugh Macdonald on 'How to Install Linux' and used that as a guide.

I find the Distrowatch.com website daunting and asked members on the Linux Space (our club 'social media' site - the Anywhere, Anytime SIG) if there is a particular version (distro) that would be better

suited to me and my hardware. Some suggested that I might find Linux Mint a good introduction to Linux without needing a lot of understanding of the basics. It is based on Ubuntu and very popular.


linuxmint

- OS Type: [Linux](#)
- Based on: [Debian](#), [Ubuntu \(LTS\)](#)
- Origin: [Ireland](#)
- Architecture: [i686](#), [x86_64](#)
- Desktop: [Cinnamon](#), [MATE](#), [Xfce](#)
- Category: [Beginners](#), [Desktop](#), [Live Medium](#)
- Status: [Active](#)
- Popularity: [3 \(2,134 hits per day\)](#)

Next I downloaded Linux Mint Cinnamon, verified the download as being complete and correct and installed it on the 250GB SSD. The plan is to install or utilise other software already installed to build up a simulation of my normal Win 10 laptop PC to check out the usability for comparison.

I found that Mint boots up very quickly and is reminiscent of Windows. The desktop is clean with a Task Bar along the bottom of the screen with a 'Start' button on the left. A very informative update-notifier in the form of a shield on the right-hand side indicates if there are any updates available. Click on the shield and a list of currently available updates to all installed apps appears allowing the selection or not of desired updates and one more click to effect the changes.

I chose to use a password to login to Mint Cinnamon. Unfortunately, I wrote it down and then changed it without noting the change. The consequence was that at the next start-up I was locked out. After racking the brains and trying all combinations and permutations without success, I did a DuckDuckGo search and found the instructions to get in and reset the password. Full marks to Linux, although it is a little scary to know that the security is so easy to foil for someone in possession of the computer.



I already use Win versions of Firefox, Thunderbird, Zoom, TeamViewer, Libre Office and VLC and

although there are minor differences in the Linux versions of programs / applications / apps compared to the Windows versions, it is easy to learn the nuances. However, getting the Linux version of Thunderbird setup the same as my Win version may be something of a chore because I have done quite a bit of surgery on the settings and layout of my Win version. However, I like a challenge.

It is pleasing to note that my Wi-Fi printer / scanner had no problems in co-operating with Linux Mint and obviously connecting to the internet was simple. Some software apps that I need, that are different to what I use in Windows, should not present any great challenges to learn. I have about three years to experiment before support is dropped for Win 10, although I expect that I will transition to seriously using Linux well before that time. As always, the internet can supply answers to most of my questions, particularly our own club Linux Space where I receive good advice and encouragement from the experts, usually within minutes of posting a question. I remember as a boy, I would thumb through a set of Encyclopaedias for answers. What a wonderful time we live in now with almost instant answers available any time of day and night!

The Tesla Optimus robot is not very impressive - but it may be a sign of better things to come

Wafa Johal, *The University of Melbourne*

In August 2021, Tesla CEO Elon Musk announced the electric car manufacturer was planning to get into the robot business. In a presentation accompanied by a human dressed as a robot, Musk said work was beginning on a “friendly” humanoid robot to “navigate through a world built for humans and eliminate dangerous, repetitive and boring tasks”.

Musk has now unveiled a prototype of the robot, called Optimus, which he hopes to mass-produce and sell for less than US\$20,000 (A\$31,000).

At the unveiling, the robot walked on a flat surface and waved to the crowd, and was shown doing simple manual tasks such as carrying and lifting in a video. As a robotics researcher, I didn't find the demonstration very impressive – but I am hopeful it will lead to bigger and better things.

Why would we want humanoid robots?

Most of the robots used today don't look anything like people. Instead, they are machines designed to carry out a specific purpose, like the industrial robots used in factories or the robot vacuum cleaner you might have in your house.

So why would you want one shaped like a human? The basic answer is they would be able to operate in environments designed for humans.

Unlike industrial robots, humanoid robots might be able to move around and interact with humans. Unlike robot vacuum cleaners, they might be able to go up stairs or traverse uneven terrain.

And as well as practical considerations, the idea of “artificial humans” has long had an appeal for inventors and science-fiction writers!

Room for improvement

Based on what we saw in the Tesla presentation, Optimus is a long way from being able to operate with humans or in human environments. The capabilities of the robot showcased fall far short of the state of the art in humanoid robotics.

The Atlas robot made by Boston Dynamics, for example, can walk outdoors and carry out flips and other acrobatic manoeuvres.

The Atlas robot, made by Boston Dynamics, has some impressive skills.

And while Atlas is an experimental system, even the commercially available Digit from Agility Robotics is much more capable than what we have seen from Optimus. Digit can walk on various terrains, avoid obstacles, rebalance itself when bumped, and pick up and put down objects.

Bipedal walking (on two feet) alone is no longer a great achievement for a robot. Indeed, with a bit of knowledge and determination you can build such a robot yourself using open source software.

There was also no sign in the Optimus presentation of how it will interact with humans. This will be

essential for any robot that works in human environments: not only for collaborating with humans, but also for basic safety.

It can be very tricky for a robot to accomplish seemingly simple tasks such as handing an object to a human, but this is something we would want a domestic humanoid robot to be able to do.

Sceptical consumers

Others have tried to build and sell humanoid robots in the past, such as Honda's ASIMO and SoftBank's Pepper. But so far they have never really taken off.

Amazon's recently released Astro robot may make inroads here, but it may also go the way of its predecessors.

Consumers seem to be sceptical of robots. To date, the only widely adopted household robots are the Roomba-like vacuum cleaners, which have been available since 2002.

To succeed, a humanoid robot will need be able to do something humans can't to justify the price tag. At this stage the use case for Optimus is still not very clear.

Hope for the future

Despite these criticisms, I am hopeful about the Optimus project. It is still in the very early stages, and the presentation seemed to be aimed at recruiting new staff as much as anything else.

Tesla certainly has plenty of resources to throw at the problem. We know it has the capacity to mass produce the robots if development gets that far.

Musk's knack for gaining attention may also be helpful – not only for attracting talent to the project, but also to drum up interest among consumers.

Robotics is a challenging field, and it's difficult to move fast. I hope Optimus succeeds, both to make something cool we can use – and to push the field of robotics forward. .

Wafa Johal, Senior Lecturer, Computing & Information Systems, *The University of Melbourne*

This article is republished from The Conversation under a Creative Commons license. Read the original article.

What is multi-factor authentication

Jongkil Jay Jeong, *Deakin University*; Ashish Nanda, *Deakin University*, and Syed Wajid Ali Shah, *Deakin University*

Data breaches are becoming commonplace in both small and big tech companies. The most recent victim was Australian telecommunications company Optus, resulting in unauthorised access to the identity data of roughly 10 million people.

Adding to the misery of the victims, this cyber-attack further unleashed a plethora of subsequent phishing and fraud attempts using the data obtained from this breach.

Having more rigorous security measures when logging in can help to protect your accounts, and significantly reduces the likelihood of many automated cyber attacks.

Multi-factor authentication (MFA) is a security measure that requires the user to provide *two* (also known as two-step verification or two-step authentication) or more proofs of identity to gain access to digital services. This typically requires a combination of something the user knows (pin, secret question), something you have (card, token) or something you are (fingerprint or other biometric).

For example, the Australian Tax Office recently tightened some rules for digital service providers on the mandated use of multi-factor authentication. If you use certain services, you're already familiar with MFA.

But not all MFA solutions are the same, with recent studies demonstrating simple ways to subvert more common methods which are used to lodge cyber-attacks.

Furthermore, people also prefer different MFA options depending on their needs and level of tech savviness.

So what are the options currently available, their pros and cons, and who are they suited for?

There are four main methods of multi-factor authentication

- **SMS:** Currently the most common option involving a one-time password (such as a code) sent via text message. Although quite popular and easy to use, the password or code texted to you can commonly be hacked by malicious apps on the phone or by redirecting the SMS to a different phone. The method also fails if your smartphone doesn't have service or is powered off.
- **Authenticator-based:** Another common method, in which an application installed on your smartphone (such as Google Authenticator) generates one-time passwords valid for a very short time span, such as 30 seconds. Although more secure than text messages, malicious apps can still steal these one-time passwords. The method also fails if your smartphone is out of power.
- **Mobile app:** Similar to authenticator apps, but a user is sent a verification prompt rather than a one-time password. This requires your smartphone to have an active internet connection and be powered on.
- **Physical security key:** The most secure mechanism; it uses a hardware security key (such as YubiKey, VeriMark or Feitian FIDO) that needs to be connected to the device to verify identity – many of these look a lot like USB memory sticks. It's the current leading method supported by companies like Google, Amazon and Microsoft, as well as government agencies worldwide.

Each of these four methods varies in usability and security. For example, despite physical security keys offering the greatest level of security, the adoption rate is the lowest, with figures suggesting only a 10% uptake.

Preference matters

Not only do different multi-factor authentication types vary in security, they also have different levels of popularity. This results in a discrepancy between the most *reliable* MFA method (the physical security key) and what is actually the most *widely used* (SMS).

Our team from Deakin University's Centre for Cyber Security Research and Innovation recently conducted a study on the adoption of MFA technologies. We surveyed more than 400 participants belonging to different age groups, educational backgrounds, and experience with MFA.

Results from our study indicate that people's preferences are impacted not just by their security needs, but also by usability. The majority of users cared most about the *simplicity* of the MFA method – this clearly explains why SMS-based solutions still dominate the landscape, even though there are safer alternatives.

In our follow-up study, users were given the most popular physical security keys for one month, to test unsupervised. Preliminary results suggest most users found the physical keys effective and intuitive to use.

However, the lack of platform support and setup instructions created a *perception* that these keys were difficult and complex to install and use, resulting in a lack of willingness to adopt.

One size does not fit all

We believe there needs to be careful consideration before any government agency or company mandates MFA, with a few key steps to consider.

Different people and organisations will have different needs, so in some cases a combination of methods could work best. For example, an SMS-based solution may be used in conjunction with a physical security key for access to critical infrastructure systems that need higher levels of security.

Additionally, user education and awareness is vital. Many people aren't aware of the importance of MFA, and don't know which methods are the safest.

By taking some personal responsibility and using highly effective methods such as physical security keys to protect our most vulnerable accounts, we can all do our part to make the web a safer place. .

Jongkil Jay Jeong, CyberCRC Senior Research Fellow, Centre for Cyber Security Research and Innovation (CSRI), *Deakin University*; Ashish Nanda, CyberCRC Research Fellow, Centre for Cyber Security Research and Innovation (CSRI), *Deakin University*, and Syed Wajid Ali Shah, CSCRC Research Fellow, Centre for Cyber Security Research and Innovation, *Deakin University*

This article is republished from The Conversation under a Creative Commons license. Read the original article.

DOTW Highlights

Roger Brown

DOTW has made the transition to SPACES

Perhaps we should first remind readers about what exactly DOTW is meant to be. Precisely what the acronym “DOTW” stands for has been shrouded in controversy over the years but in practice it is essentially a lighthearted look at some of the sillier events of the week based on nominations from members.

Members make nominations by posting in the #DOTW Nominations space preferably with a supporting URL. Nominations are confined to Australian events or the doings of Australian citizens – otherwise a certain overseas president would have won almost every week! In general criminal acts are excluded.

It’s important to remember that the poll is meant to be light hearted – when the occasional member gets nominated (even our PRESIDENT!!) it’s all in good fun.

The DOTW poll is posted in the Chit Chat space with links also posted in the All Company and #DOTW spaces, making it easy to find the latest poll at any time.

During the testing phase of Google Spaces, it appeared that a rudimentary poll facility existed and that was used to successfully post several test editions of DOTW. However when Spaces went ‘live’ we suddenly found that the poll facility became inoperative and another method of compiling the poll had to be found.

With some urgent improvisation that was done and DOTW lives on!!

And now let’s review some of the recent winners of the DOTW poll:

- Sky News Australia and the Australian newspaper who have both given substantial publicity this week to false claims that a new “international study” has found no evidence of a climate emergency in records of extreme weather!
- Victoria’s authorities responsible for the state’s Working with Children checks who administer protection laws that are the weakest in the nation.
- Victorian Supported Residential Services which according to evidence provided to the disability royal commission had residents who were routinely hungry, cold and living in unhygienic conditions.
- Former prime minister Scott Morrison who secretly appointed himself to five ministries — including Treasury, without telling the ministers concerned, far less the Australian public.
- Victoria’s government-owned logging company which illegally cleared 1,000 square metres of protected possum habitat and broke the law in 25 out of 30 logging areas, according to a government-commissioned audit.

So if YOU haven’t yet become a DOTW voting addict, do join the Chit Chat space and give DOTW a go. It’s guaranteed 100% addictive!!

Roger Brown

East SIG Report August 2022

Neil Muller

Host John Swale opened the August meeting, again via Zoom. After welcoming members, John outlined the nights agenda below:

Presentation 1: Q&A with John Hall

Presentation 2: Google Maps Tips and Tricks

Main presentation: "Ransomware Protection" by Dave Botherway

The first presentation of the night was by **John Hall** presenting Q&A in George Skarbek's absence.

1. About twice year I receive emails from 4 people I used to have contact with many years ago, one of which has passed away. I don't look at these emails, but just delete them. Could this indicate I have a problem?
2. When you receive an email make sure the email address looks genuine. Check that the email address of the sender is the actual email address that the sender uses. Sometimes scammers can spoof the address. Even if the address is correct, it's possible to make the email appear that its come from your friends address. You just need to be alert.

If your email client is setup to show a preview of the contents of an email, it's safe to look at that, so long as you don't click on anything in the email. I use Microsoft Outlook and it gives me a preview pane, so I see the contents of the email before opening it.

What's likely to have happened in your case, is spammers have got hold of your friends' email addresses and are sending you emails that purport to be from your friend. In answer to your question, I don't think you have a problem.

If your friend is deceased, just set up a rule that any emails from that address go straight to a junk folder.

1. I'm wanting to buy a good quality computer monitor for graphics work, to display lines and shapes. Unlike Smart TVs that you can go and see working at JB Hi-Fi or Harvey Norman, most stores don't have their computer monitors turned on, so you can't judge the quality of the display. Can anyone recommend a good monitor I could buy?
2. I would visit a reputable review website such as Tom's Hardware when purchasing a new monitor. Other suggestions from the audience were to visit Officeworks as they often have their monitors turned on. Another suggestion was to contact CentreCom or Scorptec to see if they have their monitors turned on before visiting their store.



Figure 1 - Computer monitors on display

15. I'm seeing advertisements for thumb drives that claim a capacity of 1TB for \$15. Does anyone know of a utility that can scan one of those drives to verify it really has that capacity?
16. The utility H2testw at <https://h2testw.en.lo4d.com/windows> is a free tool which can check your mass media devices for its actual size, as opposed to the advertised side.

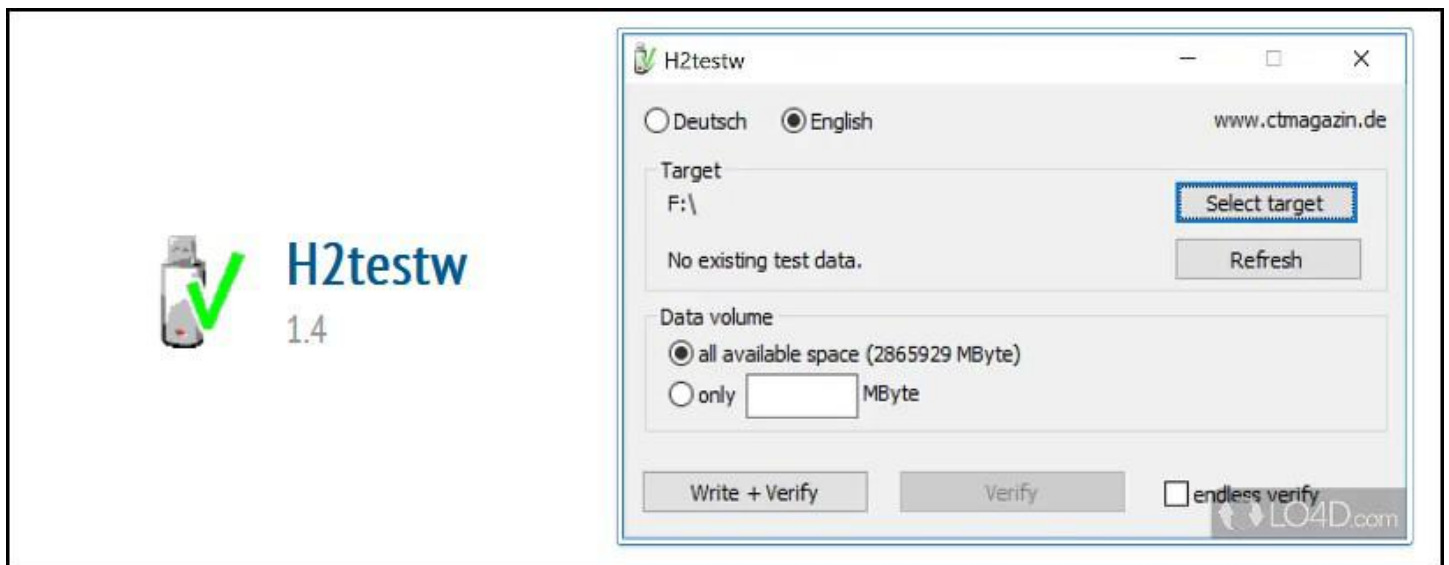


Figure 2 - Utility program H2Testw

1. I'm wanting a security camera that can read vehicle license plates at 50 metres away. It's for use on a farm and if would need to be mounted on a farm shed at that distance from the gate for its power. Does anyone know of a camera that fits the bill?
2. At 50 metres most cameras would struggle to read a license plate at that distance. Last year Stewart Bedford gave a presentation of a Eufy Cam 2C security camera that is solar powered, and one of the cameras he mounted in a tree. That may be a better option as it may be able to be mounted closer to the gate as it doesn't need power from the grid. A report of Stewart's presentation to the East SIG meeting of November 2021 appears in the February 2022 edition of PCUpdate.



Figure 3 - Eufy solar powered security camera

Following Q&A, Dave Botherway played a video by Kevin Stratvert titled "Google Maps Tips and Tricks." Kevin Stratvert is a former Microsoft senior programmer and American tech YouTuber, who uploads a wide variety of videos revolved around technology, especially Microsoft software and hardware. He has accumulated almost a million subscribers as of October 2021 and produces very professional and useful videos. The video on "Google Maps, Tips and Tricks" can be found at <https://www.youtube.com/watch?v=beeNMoXuxPg>



Figure 4 - Google Maps Tips & Tricks

Kevin's video covers 20 Google Map tips, which he demonstrates in a clear and precise manner. As most of us use Google Maps, this is a video that is definitely worth watching more than once. Rather than try to detail each tip in this report, I've listed below each of the tips and the timestamp where the tip can be found in the video.

□ TIMESTAMPS

- 00:00 Introduction
- 00:13 One finger zoom
- 00:31 Remember parking spot
- 01:11 See where you've been with timeline
- 02:14 Time travel with street view history
- 03:22 Use Google Assistant for navigation
- 04:04 Change vehicle icon on Google Maps
- 04:14 Use Custom labels for places you regularly visit
- 04:40 Save locations and share with others
- 05:19 Download and create Offline maps
- 05:53 Measure distance and area
- 07:03 Share real-time location with others
- 07:23 Avoid tolls, highways & ferries
- 07:39 View inside buildings such as Shopping centres
- 07:59 Add multiple stops to a route

- 08:17 Set a reminder of when to leave to arrive on time
- 08:55 Drag and drop to modify route
- 09:16 Public transit
- 09:40 View traffic congestion throughout the day
- 10:06 Flight prices
- 10:33 Area 51
- 10:58 Wrap up

East SIG's main presentation was on "Ransomware Protection" by **Dave Botherway**. This was a timely presentation with ransomware effecting many computer users at present, as more people are on their computers and phones due to the COVID-19 pandemic and recent lockdowns.

Dave gave a very detailed and thorough presentation, first outlining the various types off scams and ransomware current, and later websites where help is available. In this report, I've used the PowerPoint slides and information from Dave's presentation, with additional explanations where necessary.

Changes in the focus of ransomware

- **SPAM** - Spam came first and comprised of unwanted emails, which tried to sell users unsolicited products or services.
- **SCAMS** - Spam evolved into scams, with scammers seeking monetary amounts. This needed people to provide information, such as their credit card or banking details for the scammers to get their monetary return.
- **RANSOMWARE** - This is the unexpected infiltration of a user's computer by quite sophisticated techniques, by locking up the user's data. Once locked, the user is asked to pay to get their data back.
- **ASSISTANCE** - In Australia, there are many websites offering assistance to people.

Types of Scams

Investments schemes

These schemes trick people into transferring large sums of money to scammers, usually involving payment in crypto-currencies. By using crypto-currencies the perpetrators are untraceable. Third parties are used and the money returns back as "clean" money.

Business Email Compromise

False invoices received by businesses will suggest immediate payment for an account is needed. Often the invoice would be sent to clerks who may have thought the boss had overlooked payment. As payment seems urgent, it does not go through the normal auditing channels.

The scammers can often hack into email accounts and change payment detail on invoices. In these scams, the bank account detail is changed, so payment goes into their account.

Romance Scams

Romance scams target vulnerable people looking for a companion, convincing them to transfer increasing amounts of money to help their cause. These scams are usually through SMS messages so the companion cannot be identified as male or female. These scams are on the rise with people staying at home during lockdowns.

Remote Access

Scammers pretending to be from Microsoft, Telstra, NBN or your bank, will claim they need access to your computer to fix a problem. If given access to your computer as requested, they'll load remote access software onto it. Once they gain remote access, they can do anything without your knowledge. Dave indicated that like many others, he's received many of this type of scam. The latest call was around 6 hours before his presentation tonight, claiming to be from the NBN.

For the first 6 months of 2022, the monetary loss from these scams is shown in Figure 5. By far the greatest loss is due to investment scams, followed by dating and romance, then remote access scams. These figures are taken from the governments ScamWatch website which Dave covers later in his presentation.

Losses by Type (ex ScamWatch)

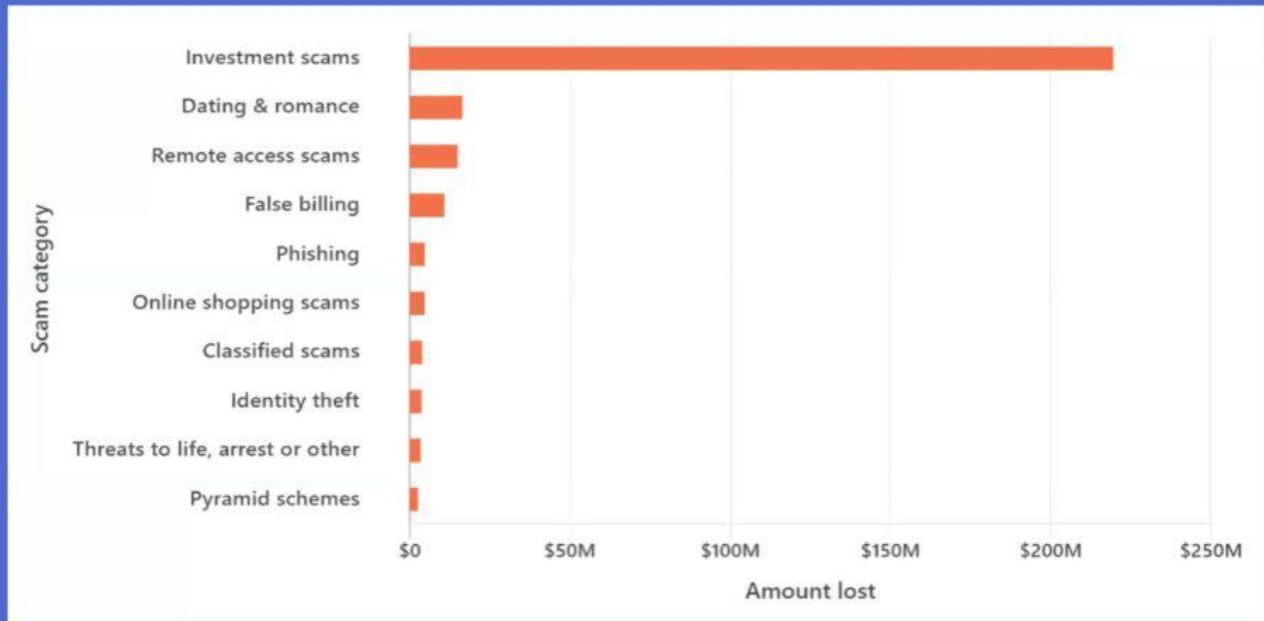


Figure 5 - Monetary Loss from Scams by Type. (from "ScamWatch").

Losses by Age Group (ex ScamWatch)

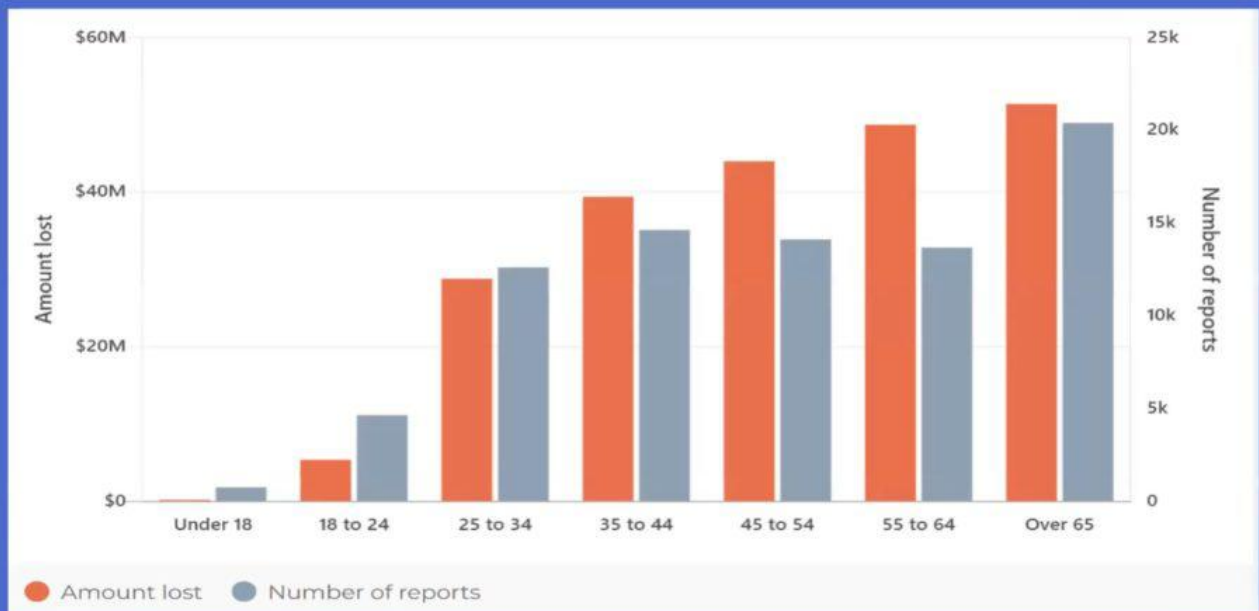


Figure 6 - Monetary Loss by Age Group

By far the greater losses from these scams are by older Australians, with the over 65 age group faring the worst. Dave was surprised that age groups 25 to 44 were as high as shown, as he felt they would have been more tech savvy. The results shown in Figure 6 were again taken from the ScanWatch website.

ACMA Impersonation scams still plague consumers.

ACMA is the Australian Communications and Media Authority and regulates the telecommunications industry.

- An alert from Australia's telecommunications industry regulator ACMA, states it is aware of ongoing reports of the following scams.**
- ACMA has warned consumers about ongoing scams where scammers are impersonating well-known telecommunications or tech companies like Telstra, NBN Co and Microsoft.**
- Receiving unsolicited calls from people saying there is a problem with your computer and offering to fix it?**
- The scammers make claims to alarm you, such as your broadband has been hacked, your computer has a virus, or there are issues with your internet or phone connection.**

Damage done by scams is more than financial

SCAMS have a truly devastating impact on their victims, wreaking havoc on their finances and emotional wellbeing. The ACCC's Targeting Scams report presents the scale and sophistication of scams in Australia. Australians lost more than \$2bn to scams in 2021.



CHRIS SHEEHAN

Each year we invest tens of millions of dollars into technology and expertise to prevent fraud and scams and protect our customers.

We use new technologies such as biometrics and have a team of experts monitoring customer accounts 24 hours a day, seven days a week to detect unusual account activity.

— using a PayID to transfer money to a person or business provides an extra check that the money is going to the intended recipient. It gives you the confidence you're paying the person you intended; and **STAY** vigilant and educated — if something looks too good to be true, it probably is. Never be pressured to pay immediately for something, or

ACCC estimates losses > \$2 bn to scams in 2021

NAB-2021: blocked > 1 Million scams targeting customers, saving / recovering > \$60 m

Besides loss of money, parallel emotional / wellbeing issues emerging . .

Figure 7 - Damage due to scams in 2021

The newspaper article Dave displayed in Figure 7 is part of a report by head of Information Security at the National Bank. The report states ACCC estimates losses due to scams in year 2021 are greater than \$2 billion. The National bank has blocked over one million money transferring scams targeting its customers, saving a little over \$60 million.

Besides the loss of money, other concerns are emerging such as emotional and wellbeing issues of those involved. Many effected don't wish to own up to being scammed. This can lead to ill feeling within themselves due to having lost so much money and some have even committed suicide.

We Have a Problem Scams

Scammers will often pretend to be 'support desk' or 'technical support' staff and ask to remotely access your computer to identify, and fix a problem. They may also ask for your personal and or financial details to pay a service fee, or ask you to buy unnecessary software as part of the fix.

ACMA warns that these scams are designed to trick you into handing over money or personal information – and *scammers may also install malware* onto your computer and request a ransom to remove it.

ACMA says that *Telstra*, *NBN Co*, *Microsoft* and other legitimate telecommunications and tech companies **will never cold-call you to tell you there's a problem** with your device or ask to access your computer.

We Have a Problem - Next Steps

If you receive one of these unsolicited calls, **ACMA advises**:

- hang up even if they mention a well-known company
- never give remote access to your computer
- never give your personal information, credit card or bank account details over the phone, unless you made the call with a phone number from a trusted source, not from the email or text message received.

If you're unsure if a call is legitimate, contact the business using contact details you've identified yourself, such as through an official website or app. More information about these scams is available on **ScamWatch** or **Cyber.gov.au** websites.

ACMA concludes: Scammers target everyone. Learn about how to protect yourself from phone scams on the **ACMA website** and make a report to **ScamWatch** if you are scammed.

The screenshot shows the ScamWatch website interface. At the top, there's a navigation bar with the ACCC logo, the ScamWatch logo, and a search bar. Below the navigation bar, there's a section titled "News & alerts" with a yellow highlight on the URL "www.scamwatch.gov.au". On the left, there's a "Scam category" table with the following data:

Scam category	Count
Attempts to gain your personal information	96
Buying or selling	85
Dating & romance	24
Fake charities	17
Investments	40

On the right, there's a news article titled "Consumers warned about fake investment opportunities as losses top \$20m". The article text states: "Losses to imposter bond investment scams have nearly tripled in the first half of this year with consumers losing over \$20 million to these sophisticated scams." The date "3 Aug 2022" is displayed at the bottom right.

Figure 8 - ScamWatch website



Figure 9 -Cyber.gov.au website

To indicate what help is available, Dave displayed webpages from the following Government websites. The ScamWatch website in Figure 8, details the different type of scams currently prevalent, while the Cyber website in Figure 9 details help and protection from Ransomware.

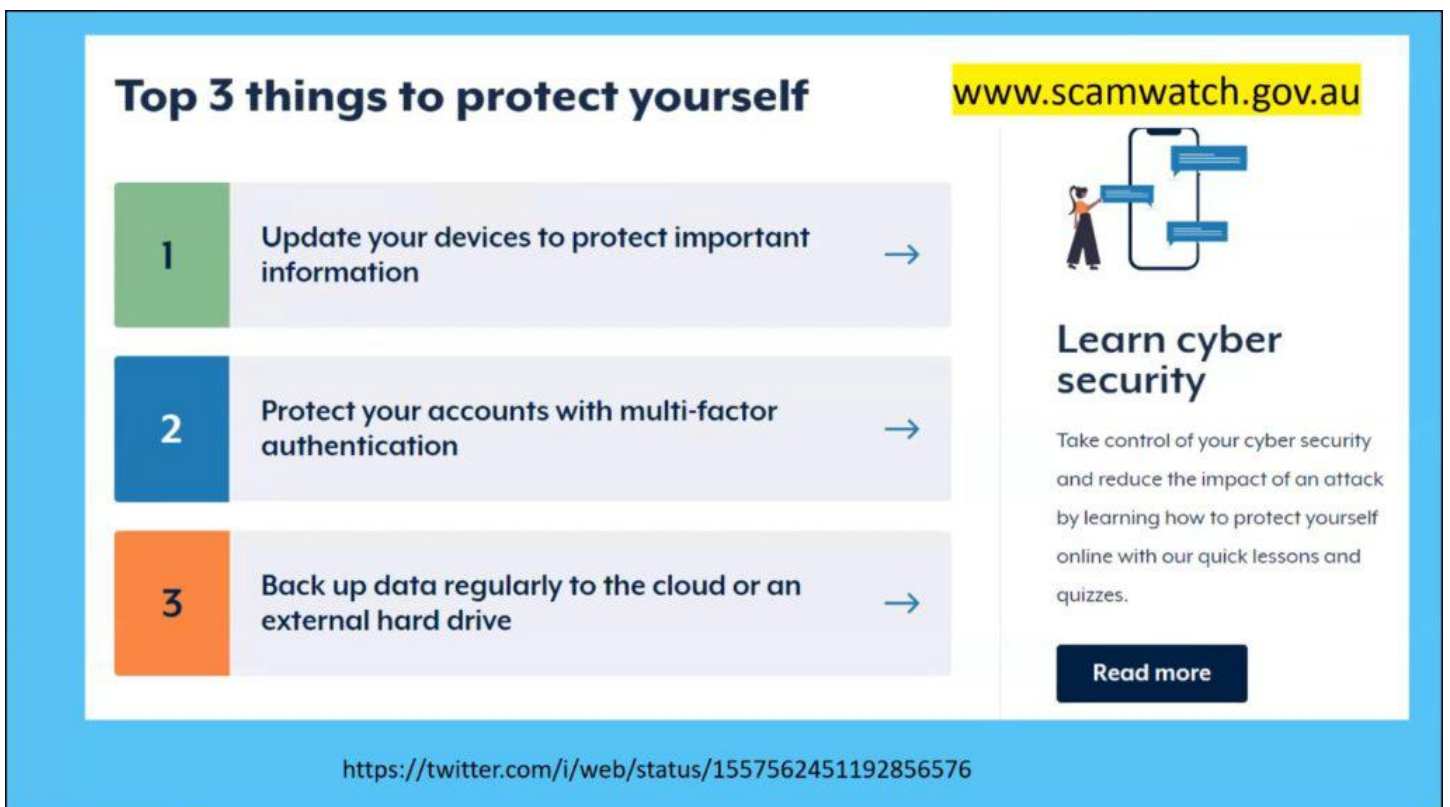


Figure 10 -Cyber.gov.au website - Top 3 Things to Protect Yourself

The Australian Cyber Security Centre has produced a useful video on ways to protect yourself which can be viewed at <https://twitter.com/i/web/status/1557562451192856576>

Below in Figures 11 and 12 are graphics from the Australian Signal Directorate's, Information Security Manual, which is available on the governments Cyber Security website. Figure 12 displays the table of contents that runs to 160 pages. Dave was impressed by the level of detail and help available in the manual, for both users and designers of corporate systems. Dave noted that hackers are no longer only going to the corporate world where the impact is greater, but targeting the small user. Although the money may not be as great, there are many more small users around the world to scam.



Figure 11 - Cyber.gov.au Information Security Manual

www.cyber.gov.au




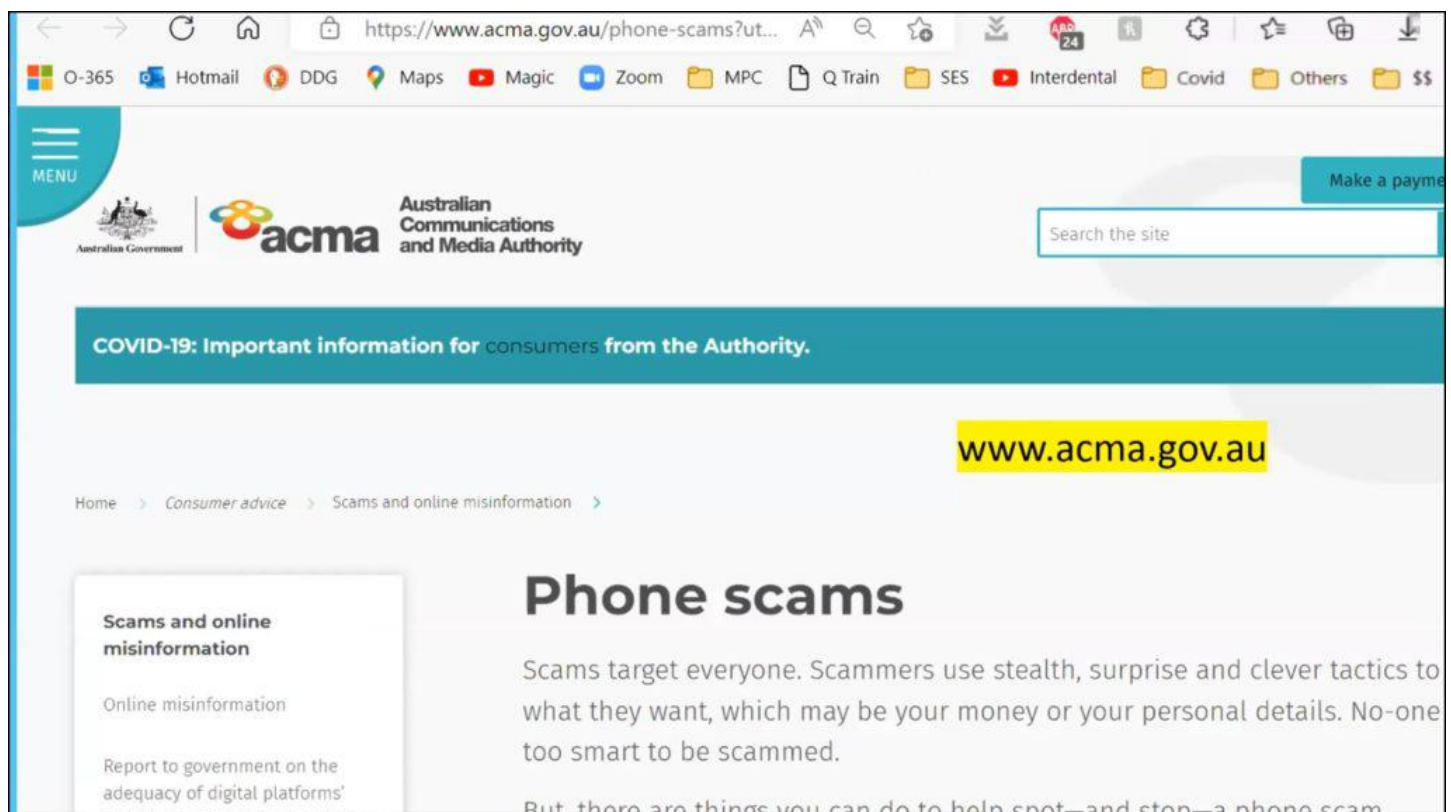
Table of Contents

Using the Information Security Manual	1
Executive summary	1
Applying a risk-based approach to cyber security	2
Cyber security	148
The cyber security framework	148
Guidelines for data transfers	149
Chief Information Officer	152
System security	153
Guidelines for data transfers	153
Cyber Security Terminology	156
Glossary of abbreviations	156
Glossary of cyber security terms	160

Figure 12 - Information Security Manual, Table of contents

Phone Scams

The ACMA.gov.au website shown in Figure 13, is more focused on assistance for phone scams. Dave found this a very good site due to the nature of information available.



<https://www.acma.gov.au/phone-scams?ut...>

ACMA Australian Communications and Media Authority

COVID-19: Important information for consumers from the Authority.

www.acma.gov.au

Home > Consumer advice > Scams and online misinformation >

Phone scams

Scams target everyone. Scammers use stealth, surprise and clever tactics to what they want, which may be your money or your personal details. No-one too smart to be scammed.

But, there are things you can do to help spot—and stop—a phone scam.

Figure 13 - ACMA.gov.au website

Below in Figure 14 is a recent cold call Dave received on his answering machine. He went along with the scammers and followed up by pressing 2 as requested. The worrying aspect of this incident, was he was unable to get through to both banks after a reasonable time and in the end hung up the call. When contacting ScamWatch, Dave felt they were more interested in assisting people who have been impacted by a scam, than being advised of a potential scam.

A recent DaveB Phone Call . . .

Female Voice . . . at 15:27, 04-August-2022

This call is from VISA Security Dept. We have seen two charges to your CC early this morning. The first charge is a \$400 bill to eBay, and the second charge is \$1,300 for an International Gift Cards mini transfer.

We believe this is suspicious and an unauthorised charge, because you have never used any Gift Card services in the past from your Credit Card.

To allow these charges, **Press 1.** To Cancel these charges, **Press 2,** To listen to these options again, Press 0

I pressed 2

Male Voice . . . Hello, Hi - Thank you for calling the VISA Cancellation Dept. How are you doing today ? . .

I hung up

I called VISA Global — they asked for my NAB Visa Card #. Told them I also had ANZ VISA CCs - they gave me the ANZ phone number and then said they would transfer me to NAB but only got silence . .

So I rang ANZ, using # Visa Global gave me	After 20 mins on hold, I hung up
I then rang NAB, using # on their website	After 32 mins on hold, I hung up
I tried to report call to ScamWatch website	But didn't have sufficient information

Figure 14 - Text from a recent scam phone call

WhatsApp Scams

Parents need to be aware of the “mum & dad” scams on WhatsApp. In this scam, scammers are posing as family members, using a different contact number, claiming their phone is broken and asking for money. They might even ask you to block or delete their old number. An example of this scam is shown in Figure 15. If you get a message like this, always call your relative on their usual number to confirm it’s not a hoax.

WhatsApp Scams . . .

Beware of 'mum & dad'
#scams on Whatsapp !

Scammers are posing as family members, using a different number & asking for money. They might even ask you to block or delete their 'old' number.

If you get a message like this, always call your relative on their usual number to confirm!



Figure 15 -WhatsApp Scam

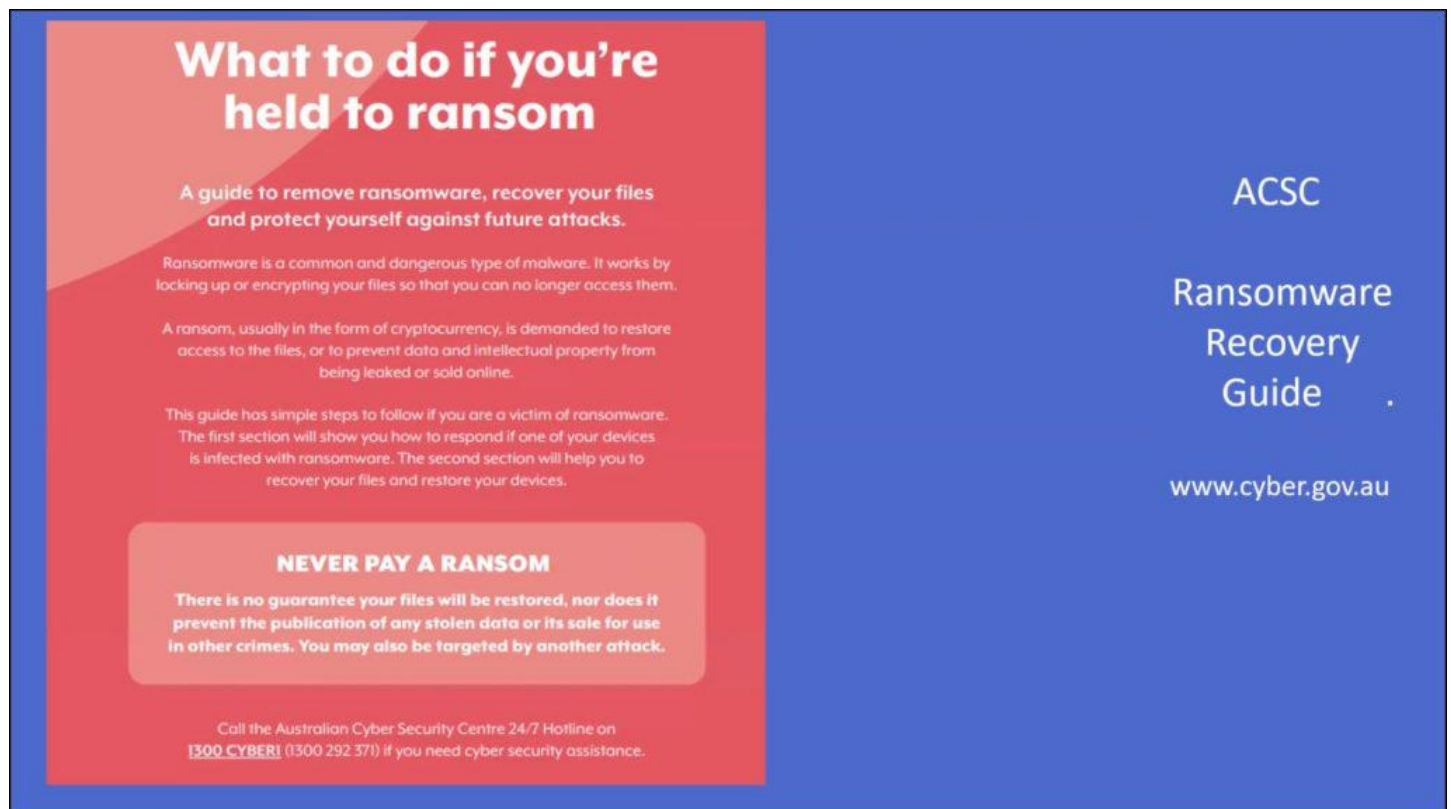
Ransomware Scams

- Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so you can no longer access them.
- A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files. Cybercriminals might also demand a ransom to prevent data and intellectual property from being leaked or sold online. A recent example of this, was in the hospital system in Victoria 12 months ago, where hospitals lost access to their computer systems and had to cease operations for a time.
- Ransomware is a growing threat as it's easy for perpetrators to try and get money.
- Once a ransom is paid, there's no guarantee you'll get data back. It's definitely not recommended paying a ransom. Once people start paying a ransom, it encourages the perpetrators to keep going.
- Ransomware can cause severe damage to both individuals and organisations. You could face significant downtime while you restore your devices and data to their original state. Firms have even gone out of business after these attacks.

- If you don't have a backup, it could be impossible to recover your files, as you need a backup before the malware was installed.
- Downtime or data loss can hurt your reputation, and cost you money.

The ACSC Ransomware Recovery Guide

A very helpful guide from the Australian Cyber Security Centre on recovering from ransomware is available from the [cyber.gov.au](https://www.cyber.gov.au) website shown in Figures 16 and 17.



The image shows a poster for the ACSC Ransomware Recovery Guide. The poster has a blue background on the right and a red background on the left. The title 'What to do if you're held to ransom' is in white text on the red background. Below the title, there is a subtitle 'A guide to remove ransomware, recover your files and protect yourself against future attacks.' followed by three paragraphs of text explaining ransomware, ransom, and the guide's purpose. A prominent white box with the text 'NEVER PAY A RANSOM' is also present. At the bottom, it provides the contact information for the Australian Cyber Security Centre 24/7 Hotline on 1300 CYBER1 (1300 292 371).

What to do if you're held to ransom

A guide to remove ransomware, recover your files and protect yourself against future attacks.

Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so that you can no longer access them.

A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files, or to prevent data and intellectual property from being leaked or sold online.

This guide has simple steps to follow if you are a victim of ransomware. The first section will show you how to respond if one of your devices is infected with ransomware. The second section will help you to recover your files and restore your devices.

NEVER PAY A RANSOM

There is no guarantee your files will be restored, nor does it prevent the publication of any stolen data or its sale for use in other crimes. You may also be targeted by another attack.

Call the Australian Cyber Security Centre 24/7 Hotline on **1300 CYBER1** (1300 292 371) if you need cyber security assistance.

ACSC

Ransomware Recovery Guide

www.cyber.gov.au

Figure 16 -ACSC Ransomware Recovery Guide.



Figure 17 -ACSC Ransomware Recovery Guide index

Identity Theft

Another website Dave highlighted was idcare.org, which assists with recovery for individuals and organisation from identity theft. Identity theft is becoming a bigger problem as people are mistakenly releasing more of their personal data in various places. This data may be aggregated by criminals from Facebook, LinkedIn etc and create a good profile to open bank accounts with that information.

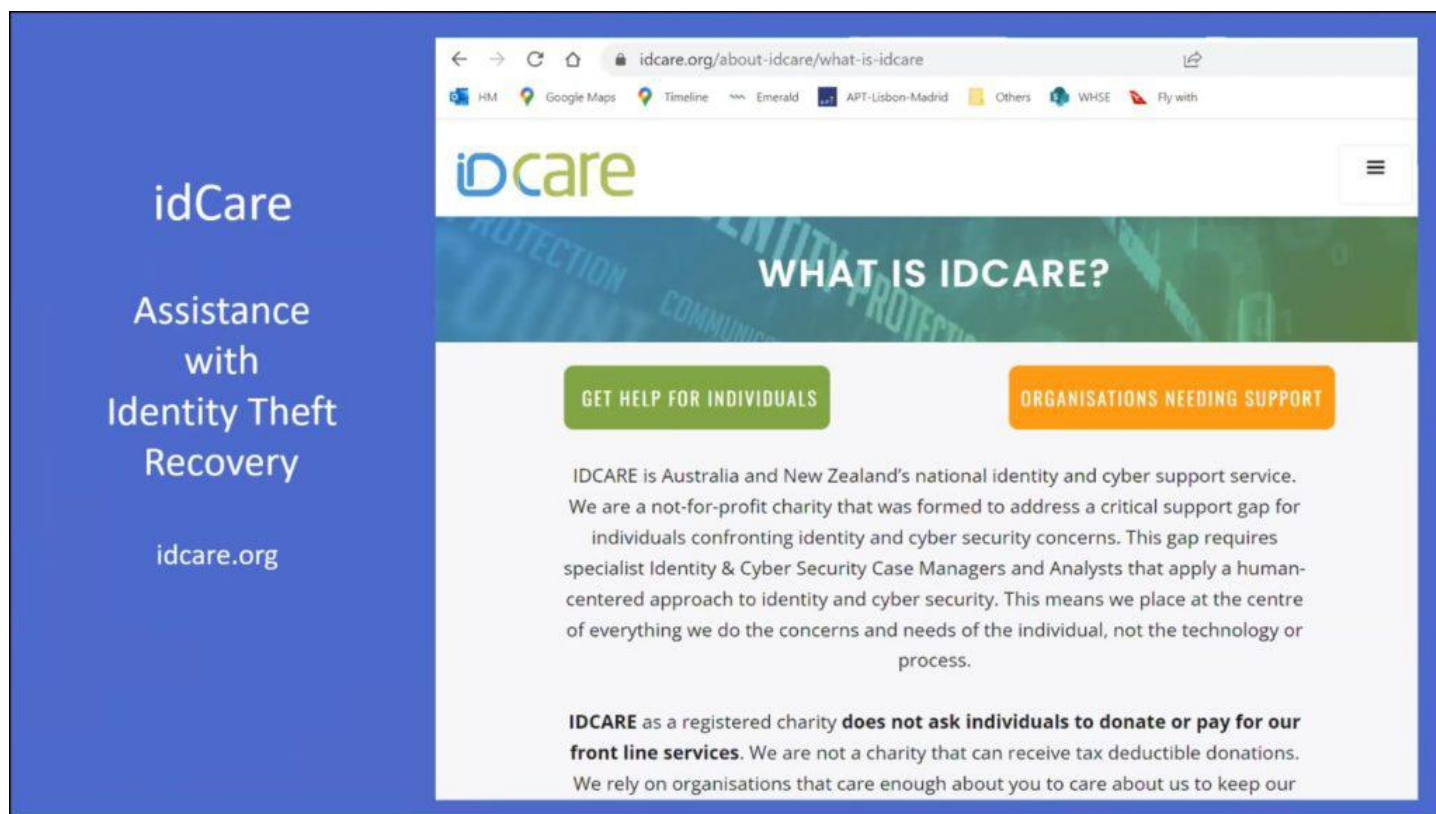


Figure 18 -idCare website

Summary

- The situation is getting worse with the volume of scams reaching users.
- Perpetrators are highly skilled, allied to the drugs trade and are after money
- Be aware of steps to minimise your risk
- Use available Government websites to assist if scammed
- Help our children, neighbours, associates who may be tricked by these scams
- Be alert – but not alarmed.



Figure 19 - Dave's Summary

Following Dave's presentation, members spoke of their own experience with the type of scams mentioned.

The following are a few useful comments made by audience members:

- A trick used by scammers to find out your name, is to ask you to "please confirm your name", rather than them asking, is this Fred speaking? If you answer that your name is Fred, they then know your real name.
- A similar tactic was to ask, "please confirm your phone number". Scammers use an automated dialling system so they normally wouldn't know your phone number until you give it to them.
- With many receiving parcels now, another scam is the text messages that your parcel has been sent and to click here to track it.
- As Dave was unsuccessful contacting his bank as outlined in Figure 14, one member said it might have been quicker to drive to the bank.
- I have been pawned https://en.wikipedia.org/wiki/Have_I_Been_Pwned%3F