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.

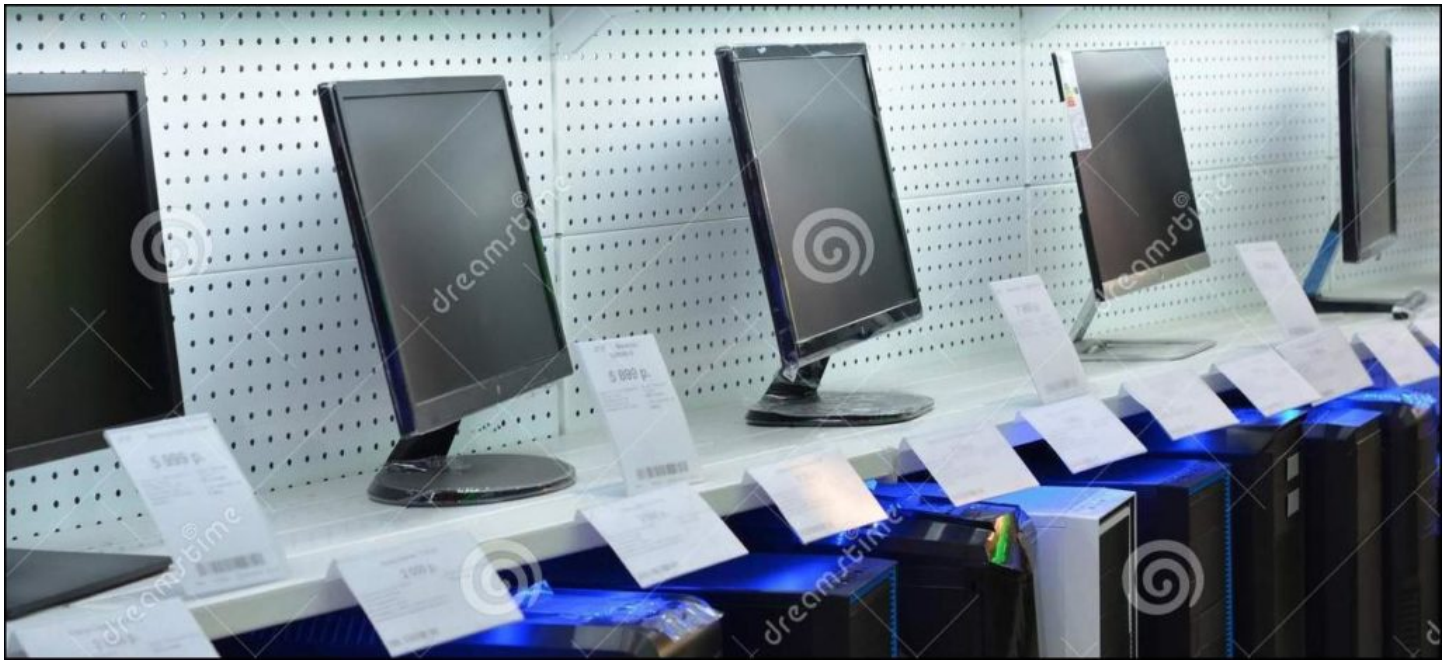

Figure 1 – Computer monitors on display

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.

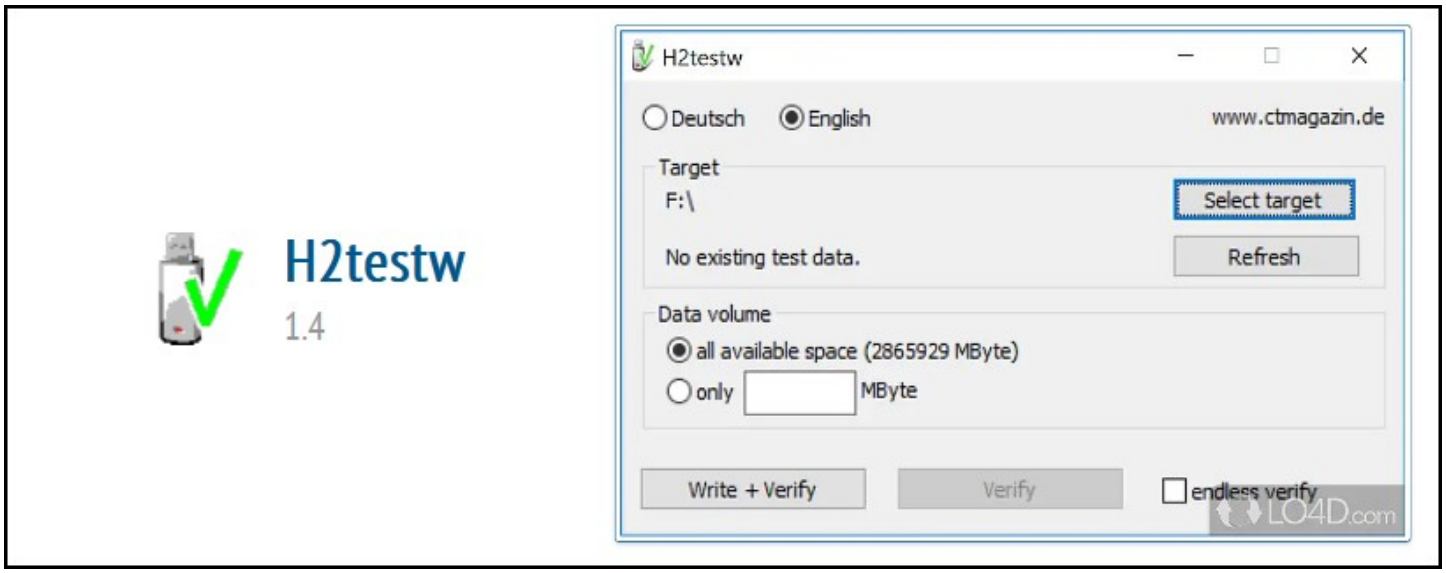

Figure 2 – Utility program H2Testw

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.

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

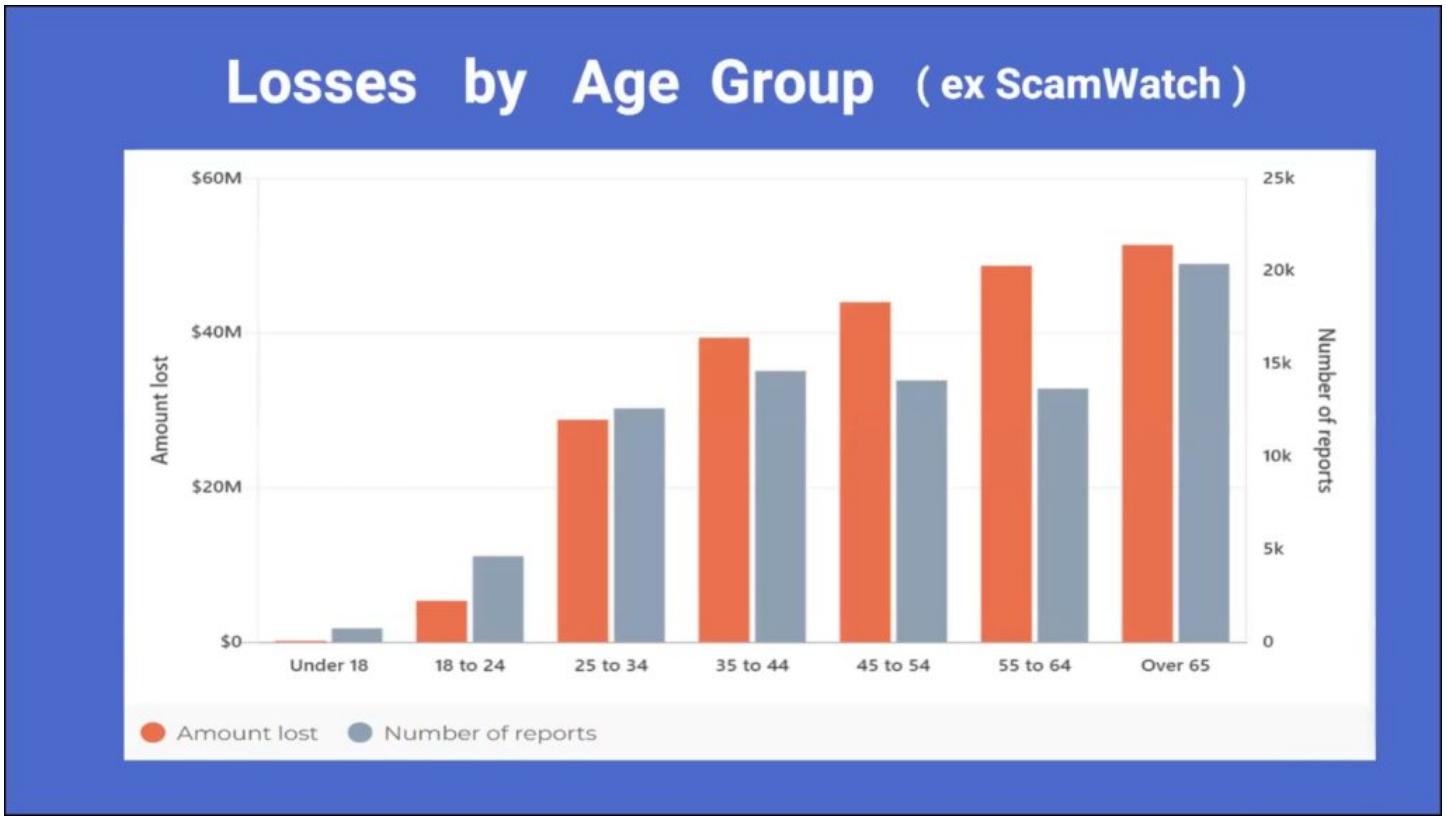

Figure 6 – Monetary Loss by Age Group

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.**

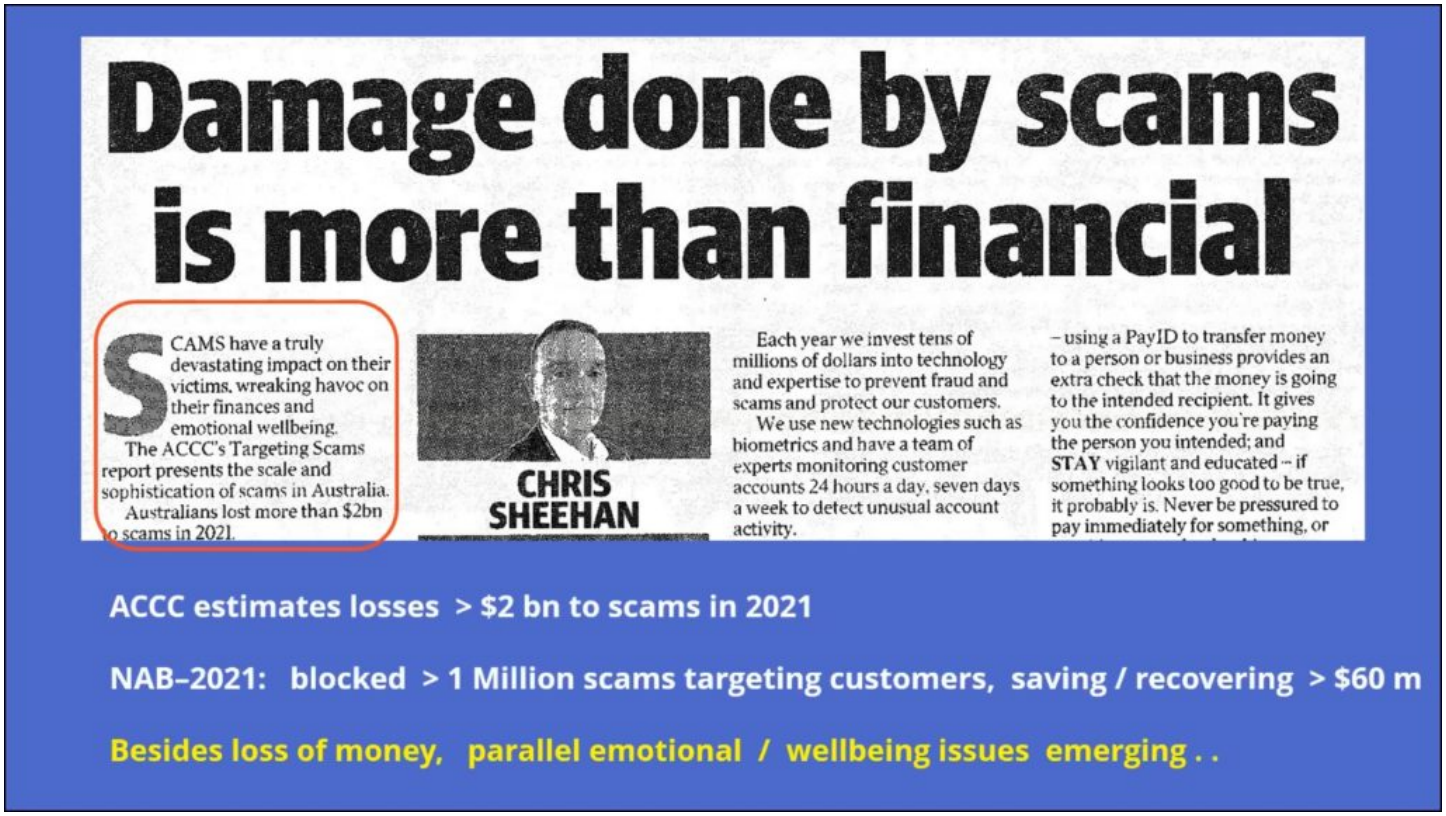

Figure 7 – Damage due to scams in 2021

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.

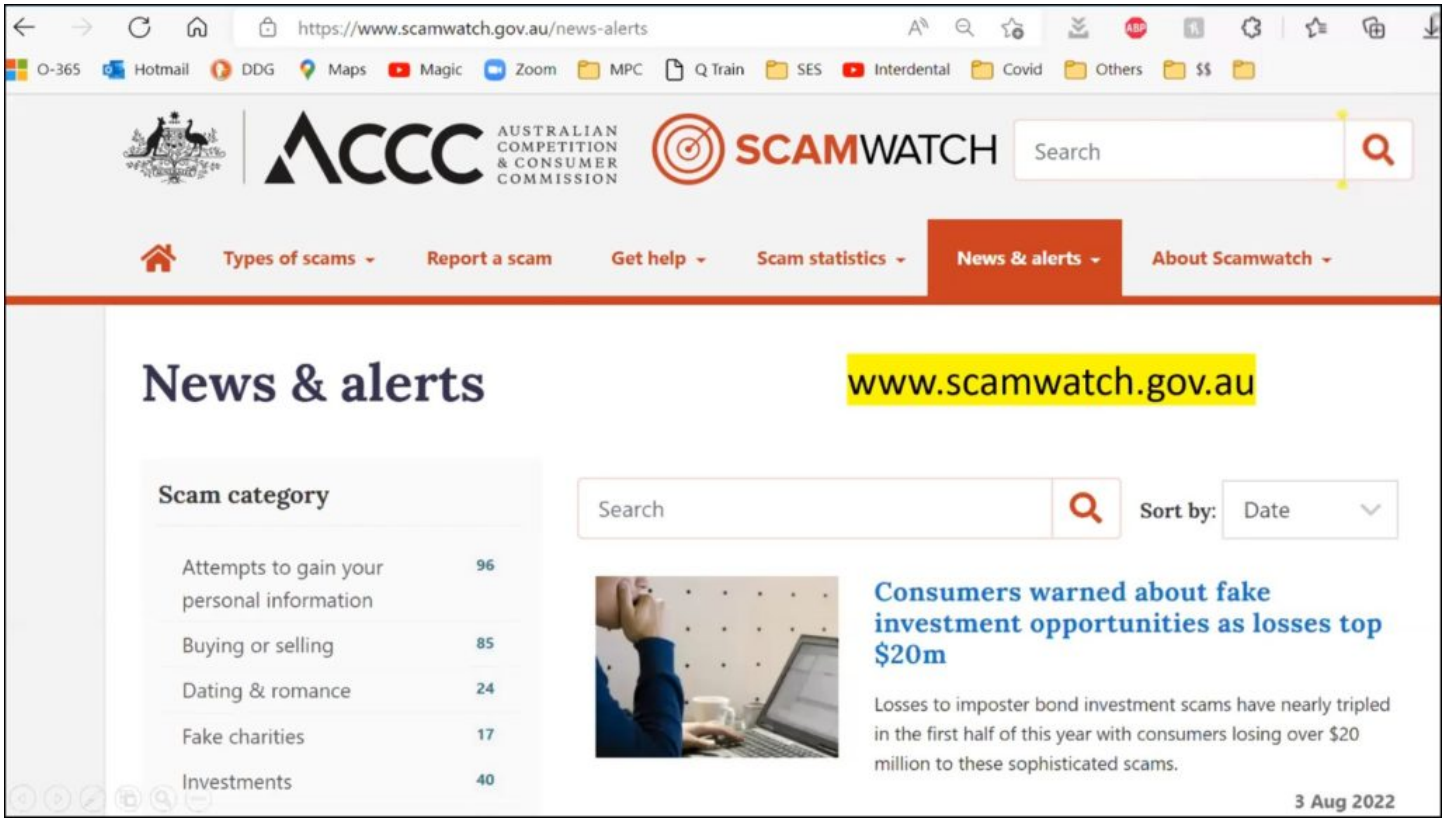

Figure 8 – ScamWatch website

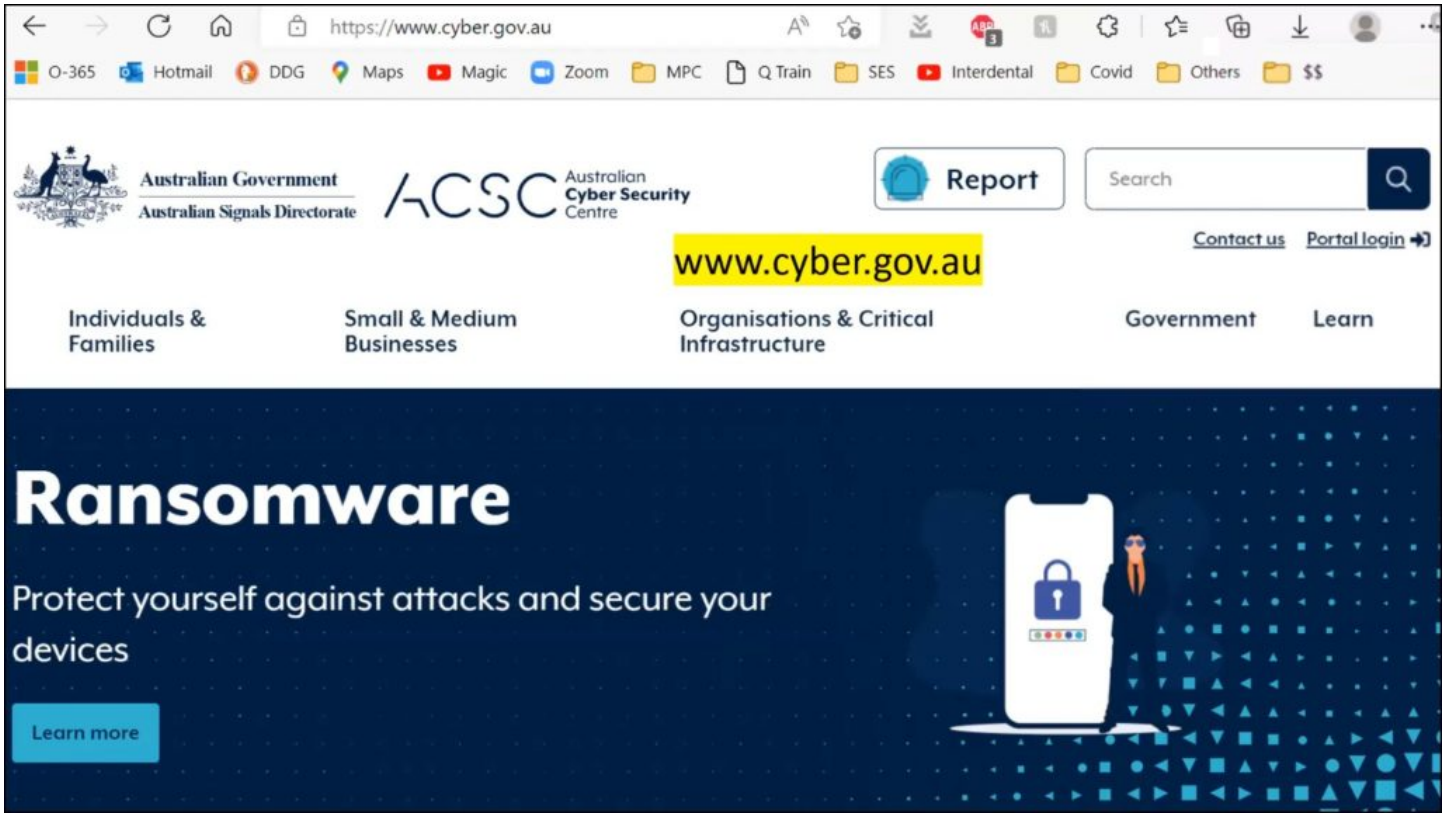

Figure 9 -Cyber.gov.au website

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

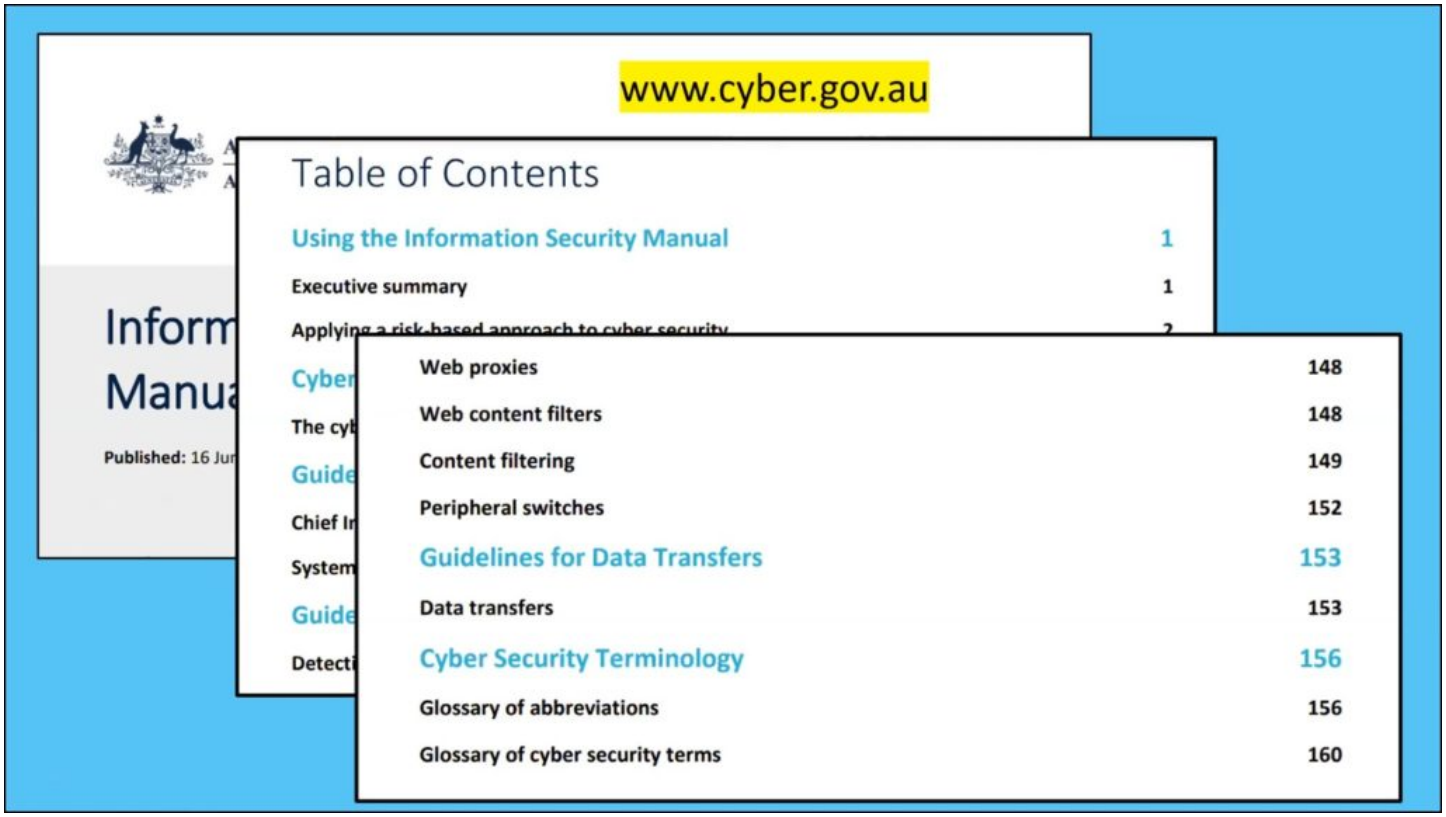

Figure 12 – Information Security Manual, Table of contents

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.

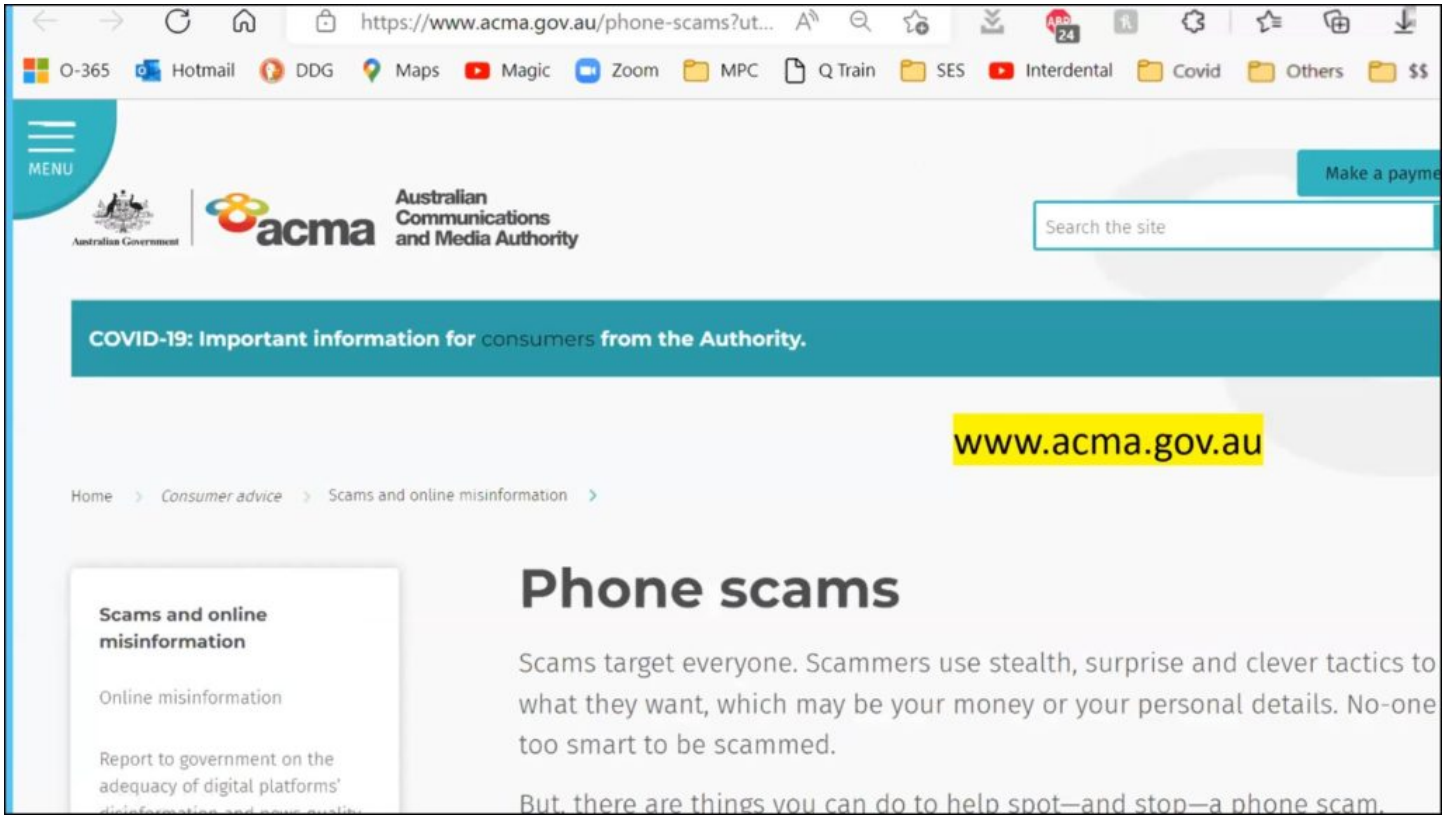

Figure 13 – ACMA.gov.au website

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.

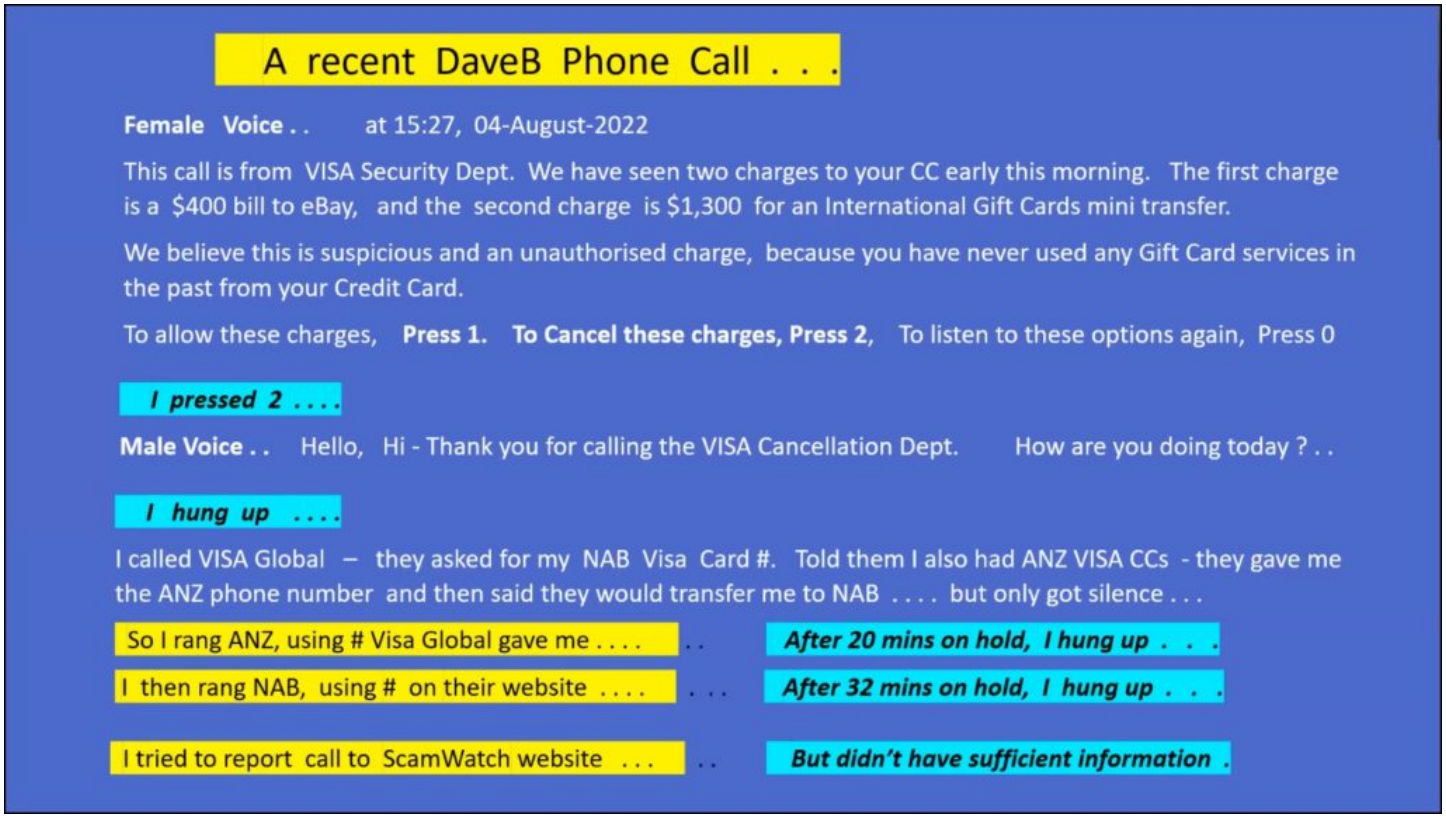

Figure 14 – Text from a recent scam phone call

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.

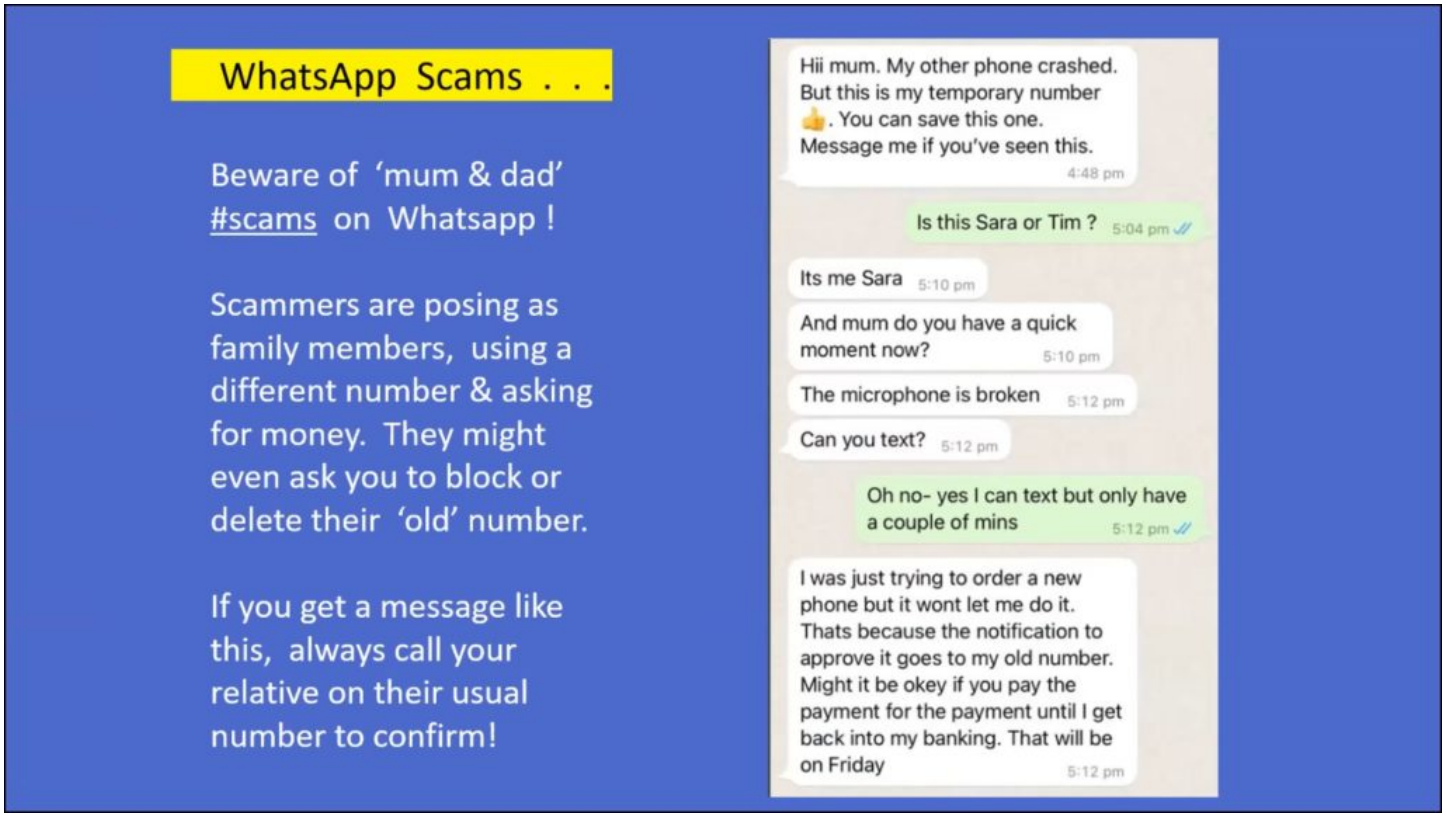

Figure 15 -WhatsApp Scam

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 Ransonware Recovery Guide

A very helpful guide from the Australian Cyber Security Centre on recovering from ransomware is available from the cyber.gov.au website shown in Figures 16 and 17.

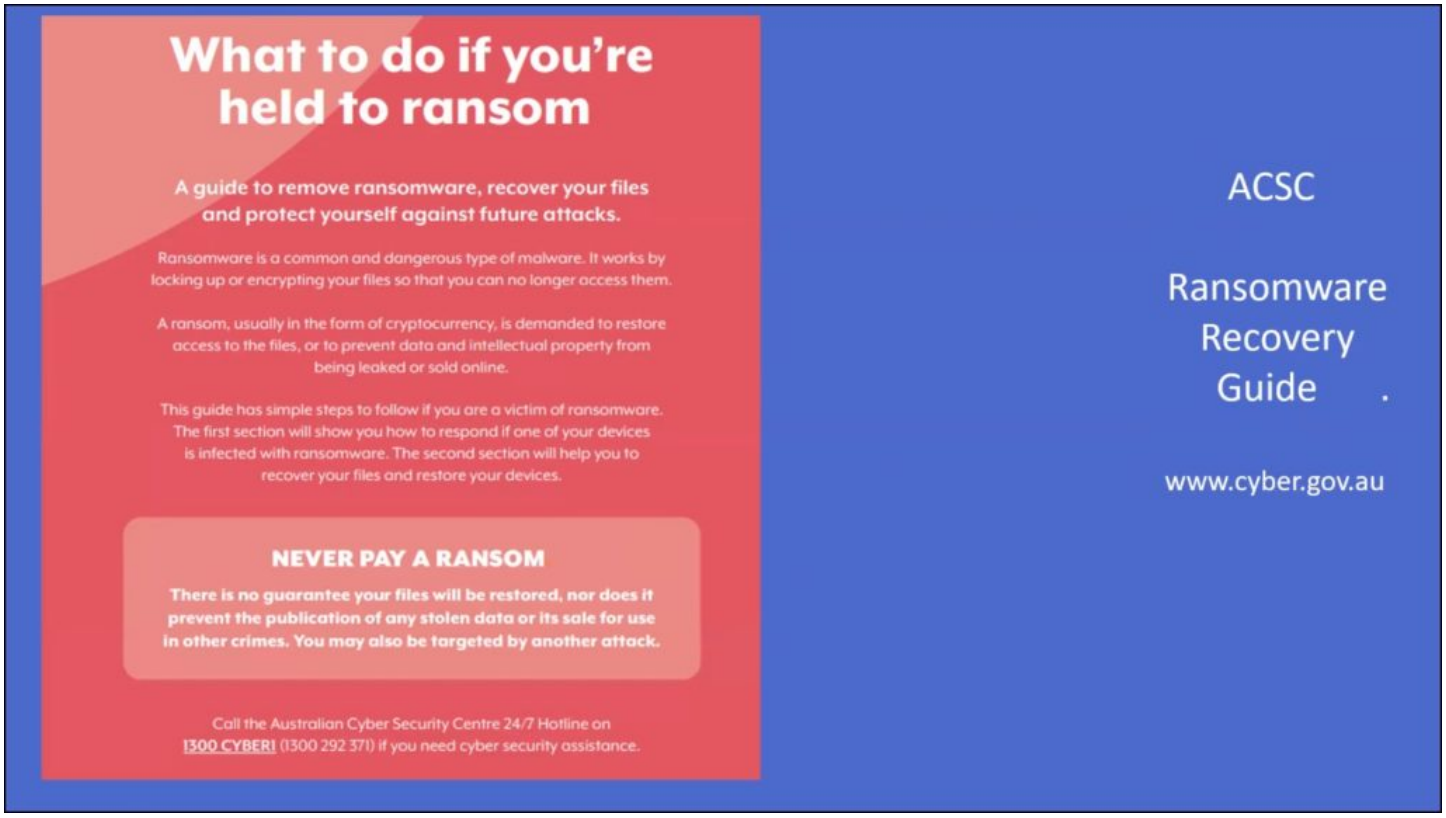

Figure 16 -ASCS Ransomware Recovery Guide.

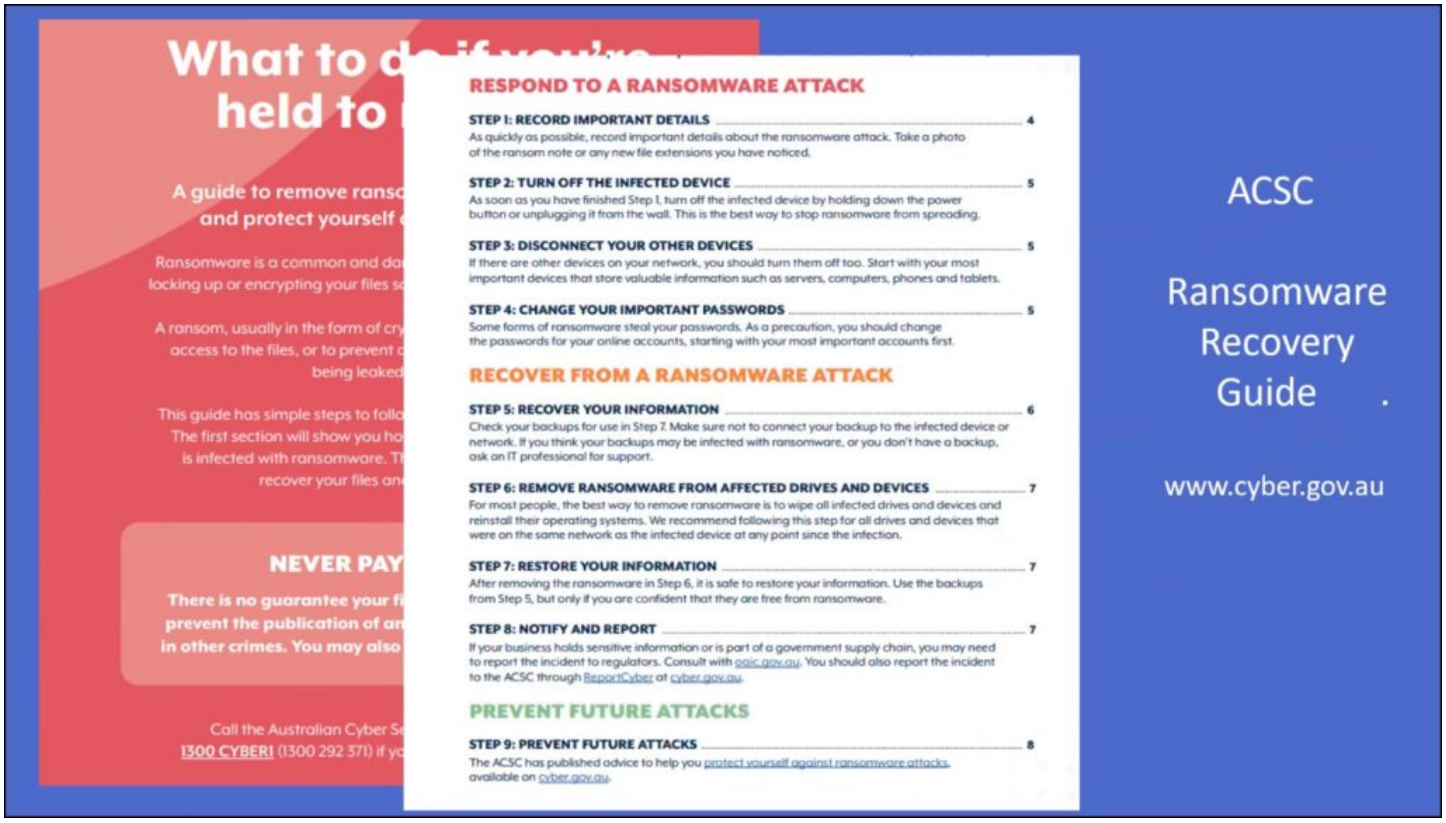

Figure 17 -ACSC Ransomware Recovery Guide index

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.

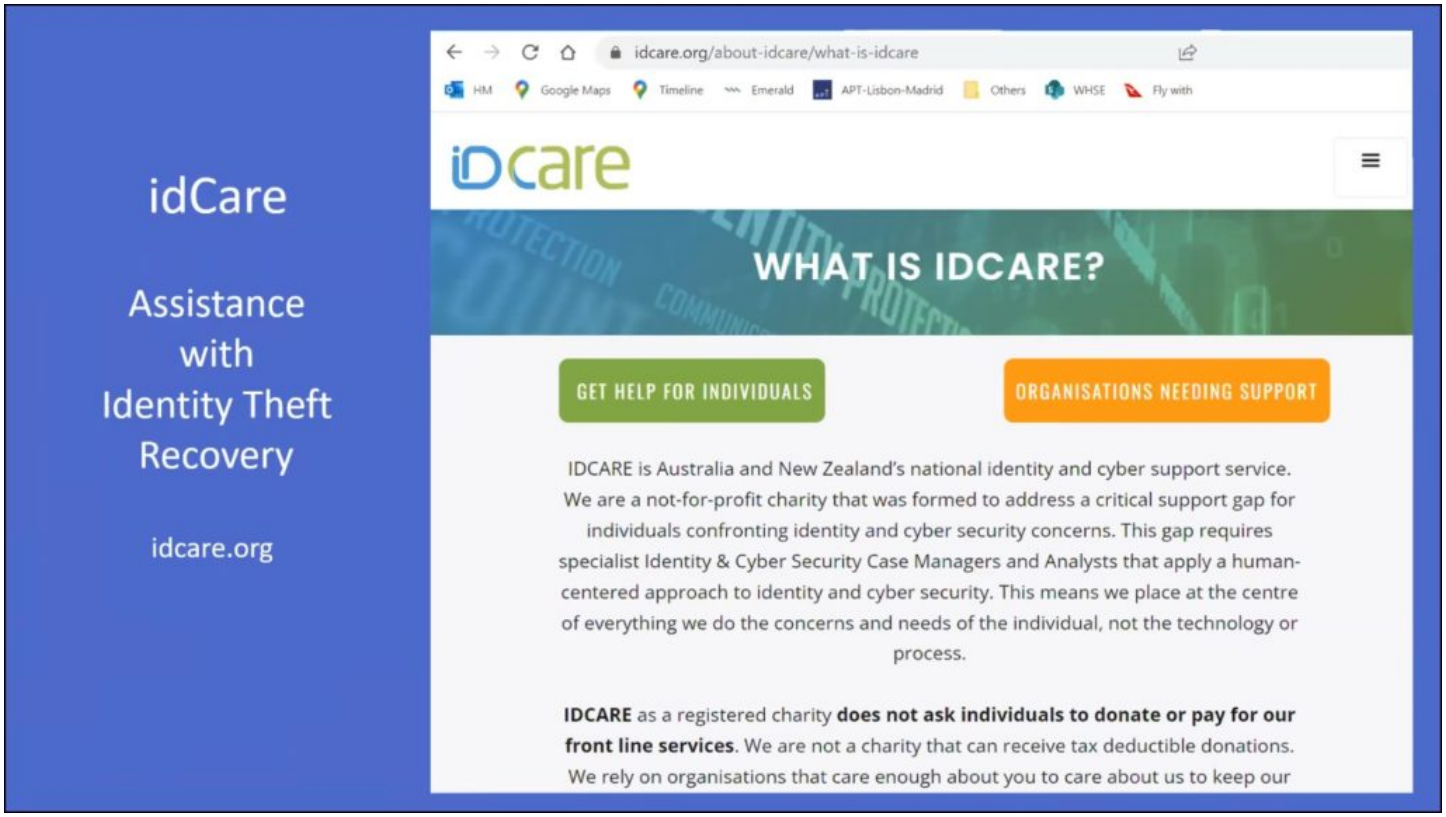

Figure 18 -idCare website

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