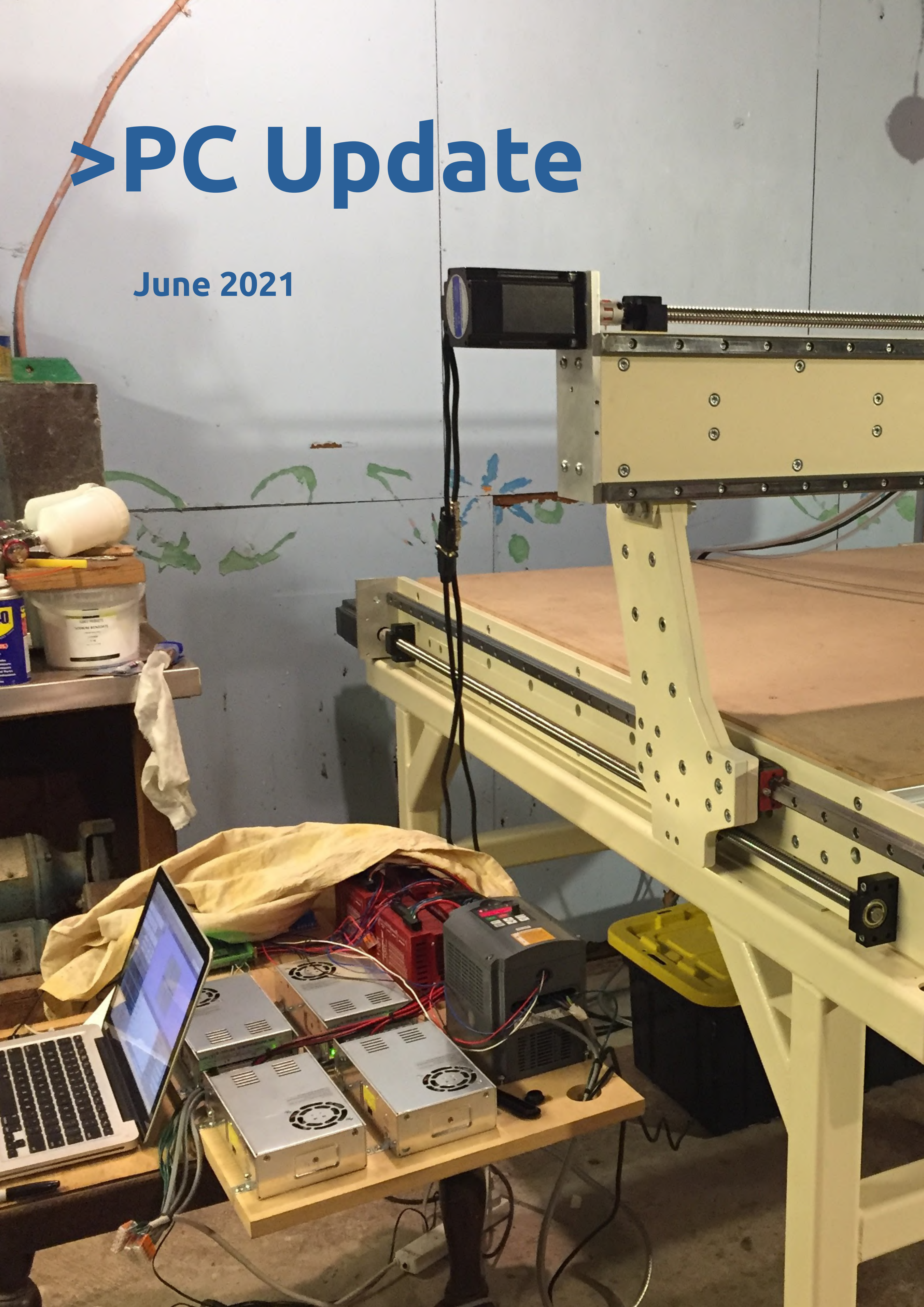
>PC Update

June 2021



Publishing Information

The newsletter of

Melbourne PC User Group

Suite 26, Level 1, 479 Warrigal Road Moorabbin 3189

Office hours 9.30am – 4.30pm (Mon-Friday)

Email office@melbpc.org.au

ABN 43 196 519 351

Victorian Association Registration A0003293V

Editor Hugh Macdonald (editorpc@melbpc.org.au)

Technical Editors Roger Brown, Kevin Martin, Dennis Parsons, Malcolm Miles

Proof Readers Harry Lewis, Tim McQueen, Paul Woolard

Librarians Malin Robertsson (office@melbpc.org.au), Choy Lai (cplai@melbpc.org.au)

Committee David Stonier-Gibson (President), Stephen Zuluaga (Vice-President), Aidan Kelly (Secretary), Peter McConnachie (Treasurer), Peter Boin, Rob Brown, Stewart Gruneklee, Paul Hattam, Harry Lewis, Hugh Macdonald (committee@melbpc.org.au)

Melbourne PC User Group Inc. is a member of the Association of Personal Computer User Groups

iHelp – Get the help you need with your computer, Ph: (03) 9276 4088,

Email: ihelp@melbpc.org.au, Live Chat!, Online Support Request

Online membership form

Responsibility for content in this newsletter lies with individually named authors

Please remember to always bring your membership card to meetings

SIG Listings and up to date calendar are available on our homepage

Editorial June 2021

Hugh Macdonald

Welcome to the June 2021 edition of PC Update.

As Melbourne has once again found itself in Covid lockdown, there is not a lot to report this month from a club perspective. The Monthly Meeting transitioned back to an online format and was a lively discussion with David Stonier-Gibson, Kirsten Ellis and Nathan Sherburn which all in attendance thoroughly enjoyed.

From the point of view of the magazine, after last month publishing an article on backing up using some ancient Windows tools, this month I've written up an article on the best way to back up for your operating system. All three major operating systems are covered, even Mac OS.

We've also got some handy tips on blocking unwanted emails, which apply to the new MelbPC Google Workspace service which you may have been transitioned to by now.

We've also got Part 2 of Dave William's fantastic project to build his own CNC Router. If you read Part 1 last month, make sure you read Part 2.

Some of the usual features are also along this month: Interesting Internet Finds, DOTW Winners, Yammer Highlights and the East SIG Report.

Happy reading!

Monthly Meeting June 2021

The June 2021 Monthly Meeting was held online on Wednesday 2nd June 2021, with almost 100 members in attendance via Zoom. This was the program for the evening:

Guest Speakers: Dr Kirsten Ellis, Nathan Sherburn
Panel discussion “Learning in Lockdown” moderated by David Stonier-Gibson

Dr Kirsten Ellis

Dr Kirsten Ellis is lead of the Inclusive Technology Group in the Faculty of Information Technology at Monash University, is a Superstar of STEM and Inventor of TapeBlock. She is enthusiastic about using technology to create a more inclusive society. She brings together technology and creativity to produce innovative solutions to real world problems. Her research interests include human computer interaction where she utilises her experience in designing, developing and evaluating systems for people to advance the field of inclusive technologies

Nathan Sherburn

As CEO of FLUX, Nathan spends his time working with educators around the world to find new and innovative ways to amplify teachers’ knowledge and experience and increase the level of engagement and interactivity in classrooms. Before FLUX, Nathan spent four years working on a PhD in education technology but dropped out to build his vision for the future of learning. In his spare time, he enjoys reading about long-termism, Effective Altruism, moral philosophy, and existential risks.

FLUX is a Melbourne-based start-up on a mission to make teaching and learning interactive and fun. FLUX provides teachers with a one-click-solution for live polls, Q&A’s, feedback and more. Since its first release just a few years ago, the FLUX platform has been used by more than 4,000 teachers and 100,000 students – with over 4.9 million unique responses from students to date.

Meeting Agenda

7.00pm sharp: Meeting opens. Host is Peter Bacon.

Guest speakers: Kirsten Ellis, Nathan Sherburn with David Stonier-Gibson

Social break.

Audience choice videos chosen by Flux poll.

President’s Report: David Stonier-Gibson.

iHelp Online: Harry Lewis and iHelp Team.

9.00pm (approx): Close.

If you missed out the first time and would like to view any of these presentations, you can do so at http://services.melbpc.org.au/videos/

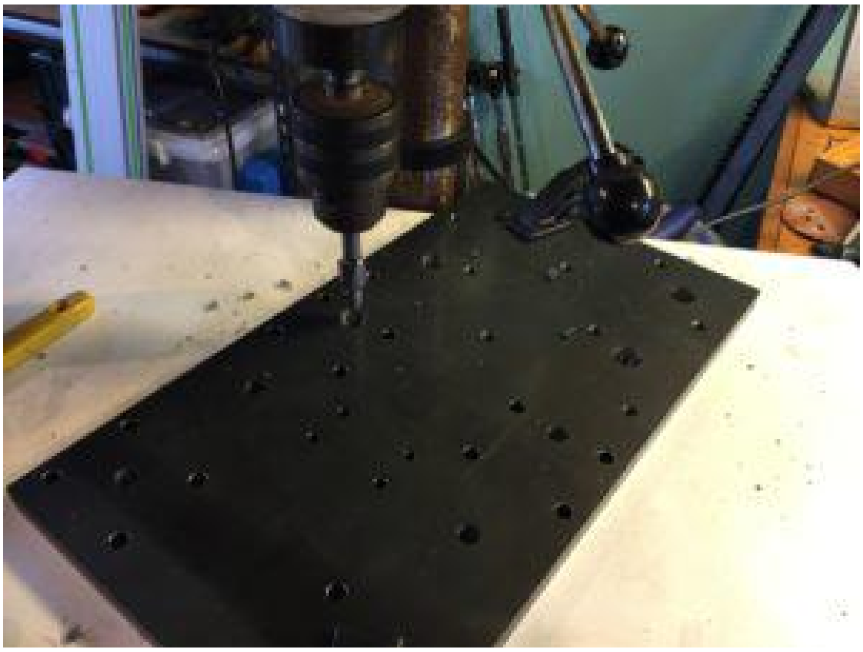
The username is videos and the password is drum286.

Building a CNC Router (Part 2)

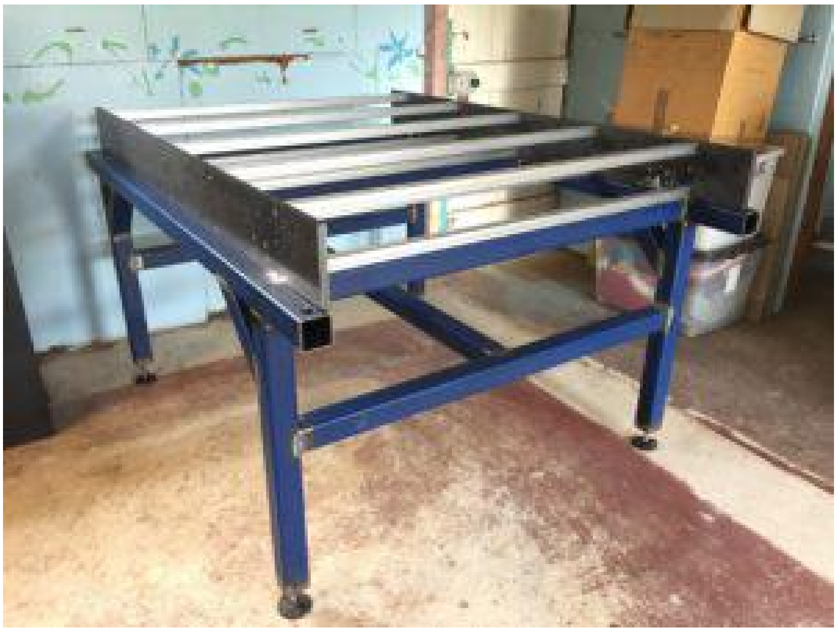
Dave Williams

This is the second part of a series of articles on Dave Williams' experience of building a CNC (computerised numerical control) router, which is an automated cutting machine that can be used on materials such as wood, composites, aluminium etc.

The laser cutting place was able to cut the steel and do the tapping for me, but they couldn't do the counterbores, so I had to begin this relatively 'boring' process:



Here is the concept for how the base works; The two side plates are held parallel and straight by these aluminium profile pieces (which I will have to reinforce soon, but it should be rigid enough to get started). The two side plates are also bolted down to the base frame and can be adjusted and shimmed to make the two linear rails 'planar' if & when necessary:

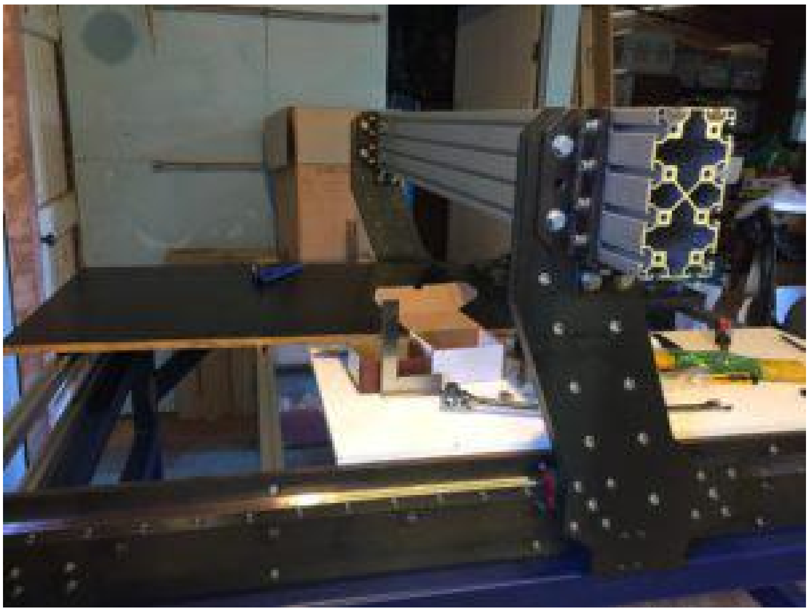


I've been using one of those laser levels to get it all level & planar to within a millimetre or two, I'll see if I can come up with any other ways to get it even more accurate in future.

I’ve been doing a lot of ‘dry fit’ stuff with this build. It slows me down, but it’s nice to see it at least partially assembled as a kind of reward for all the mental (and physical) effort. I will need to dismantle it all again to get the various steel parts primed and painted, but I’m also becoming intimately familiar with how everything fits together, so that should be helpful with future maintenance and upgrades.

There are many things that I’ve glossed over here that did crop up throughout the process so far. For example, the linear rails were all too long, so I had to carefully cut them down with an angle grinder. The ball screws were machined to the exact right length, but the shoulder that fits in the fixed / driven bearing housing were too tight for me to get them on, so I had to set up a jig with a hand-drill and carefully lap them down with some wet and dry sandpaper. The steel plates are all a bit bowed, but luckily the way it’s constructed, that bow gets straightened when everything gets bolted together – for the gantry arms, I was able to place the inner and outer plates with an opposite bow and by bolting them together the bow was cancelled out. There is one plate (The X-Axis Carriage) that doesn’t have anything to straighten it, so I will be attempting some ‘flame straightening’ methods with a boilermaker friend who has an oxyacetylene set. Look up flame straightening, it’s a fascinating technique, and able to correct (or create) some quite extreme bends in steel!

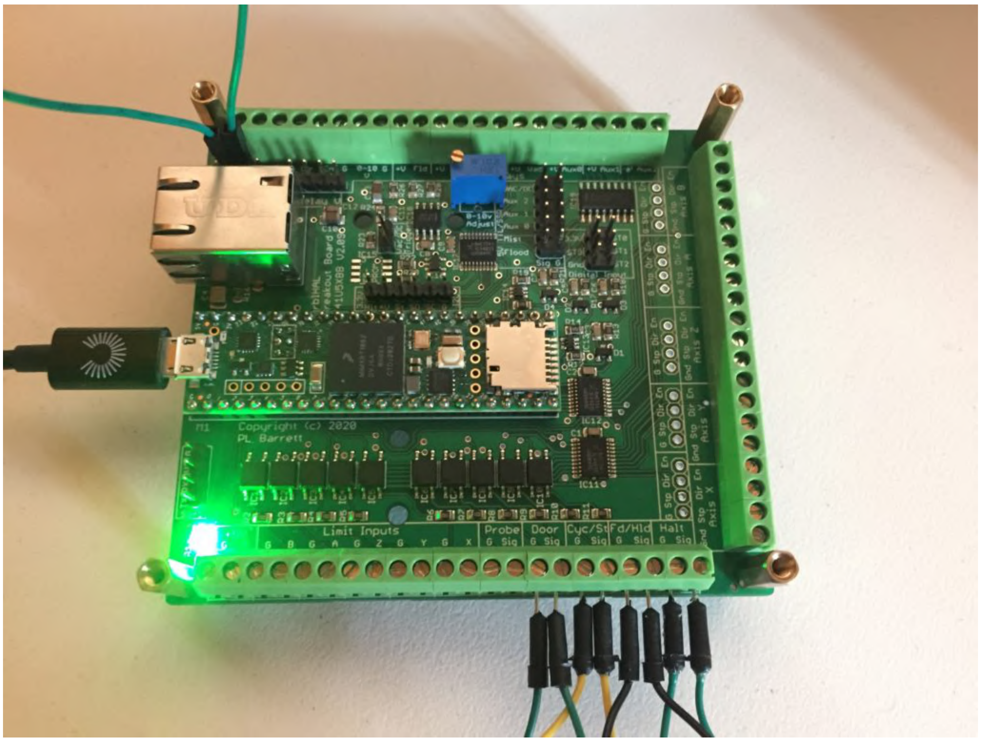
The gantry aluminium profile arrived the other day (finally), and so I’ve been able to get the whole gantry assembly put together as a dry fit:



It will all be driven by some closed-loop stepper motors with a decent amount of torque (9 & 12NM), because the gantry is rather heavy with all that steel. The spindle is a 2.2KW water cooled model and should be variable speed control via the software / g-code.

And that’s got us up to date with where I’m at!

I’ll be running everything with open-source firmware / software. I’ve sourced a control board / motion controller that is based on a more updated version of grbl called grblHAL (HAL stands for Hardware Abstraction Layer), so it can run on a whole variety of different microcontrollers. The Arduino nano version of grbl was maxed out in terms of capability (and memory!), and I wanted something that could be fourth-axis compatible in future.



Based on a Teensy 4.1 MCU, and all manner of opto-isolated inputs and outputs included, also an ethernet interface, which I’ve yet to get working, but hopefully will allow a robust EMI resistant connection to the computer. It’s all open source and wasn’t expensive, considering how much CNC breakout boards can typically cost.

I have a couple of gcode senders to try out (like UGS), with varying levels of capability, and I did also manage to get a PC-only one sucessfully talking to the board from inside a windows VM set up via VirtualBox.

To be continued…

Best Practice Backups for your Operating System

Hugh Macdonald

Last month in *PC Update* we published an article by Dan Douglas on backing up in Windows. While this presented a method that would work if members followed the advice, there are more up to date methods that can be used. Also members of Melbourne PC User Group use other operating systems like Linux and Mac OS, and so this month we present the best practice you can use on each operating system for backing up your computer.

Linux

No matter what Linux distribution you use, Linux includes a tool called rsync that makes it easy to keep the contents of one location in sync with another location. These locations can be remote from one another (copying from your computer to another computer, or from your computer to a NAS [networked attached storage] device) or local to each other (copying from one drive on your computer to another drive on your computer). Each time rsync runs it will ensure that both locations are a mirror of one another.

Rsync is executed from the command line in Linux and it can then be scheduled using cron (a cron job) at whatever frequency you find desirable.

Of course, if you are a fairly new Linux user then you may not be too keen on touching the command line. If you fall into this category then there is a utility called Back In Time that provides a graphical front end to the rysnc command and helps you create a cron job. Most distributions include this program in their repositories, so you can just search in your package manager (software store) to install it.

When it comes to restoring in Linux you don’t need to restore your whole system. The best practice is to reinstall your distribution, reinstall your applications (so keep a list of the applications you do use and the relevant package names) and then restore your Home folder. This simply requires reinstalling Back In Time, selecting the snapshot and then running the restore process. Restoring your Home folder will restore all the settings for your applications so you’ll be up and running again after this.

Another option you can use for Linux is Deja Dup. This will also backup your Home folder on a schedule in much the same way that Back In Time will. The other feature that Deja Dup offers is the ability to backup to Google Drive, which gives you the added peace of mind of having your backups located off site easily. Deja Dup is also available in the repositories of most Linux distributions. So try out Back In Time and Deja Dup and see which one you prefer.

Mac OS

If you are a Mac user then your best solution is Time Machine, which is built into the operating system. Time Machine takes regular backups of your entire drive (usually at hourly intervals) when the computer is on. It is pretty much set and forget, and once you have configured it, you only have to ensure that a backup drive is connected to the computer or the NAS or Time Capsule is powered on and online.

Restoring individual files on a Mac involves entering the Time Machine. To do this, you need to firstly open Finder and navigate to the folder that you want to restore files to. Then you need to click on the Time Machine icon in the upper right section of your screen and from the menu that appears choose ‘Enter Time Machine’. This will bring up the Time Machine interface that will enable you to navigate back in time until you see the files that you are wanting to restore. Then you simply select them and press Restore to begin the process.

If you need to restore your whole system on a Mac, or even migrate to a new Mac, within the standard installation process for Mac OS there is an option to restore from a Time Machine backup. You simply select this and the Mac OS installer will copy your applications, documents and settings back and you will end up with your system being how you remember it.

Windows

When it comes to Windows, unfortunately it isn't as organised as Mac or Linux when it comes to the separation between applications, settings and documents. So really the only way you can restore a fully working system easily is with an image backup. If you only backup your User files then you will have to reinstall Windows, reinstall all your applications (which can be time consuming using individual install processes if you have a lot of applications), and then restore your User files. So the best solution is to use an image backup, which takes a snapshot of your entire hard drive each time you run it. My favourite application for doing this is Macrium Reflect.

Macrium Reflect is free for non-commercial use. To use it you simply select your hard drive, choose that you want to create an image of it, and then go through the setup routine which will prompt you to set a schedule for performing full images (i.e. if your hard drive is 280gb then this image file will be 280gb) and differential images (if you've changed 10gb of files since your last backup then this image file will be 10gb). You can setup Macrium Reflect to backup to an external hard drive or to a NAS (networked attached storage) device.

When it comes to restoring from Macrium Reflect, if you want to simply restore a few files that you have lost then you can use the program to mount your most recent image backup as a hard drive you can access in Windows Explorer. From there you can simply navigate to the folders and files you need and copy them back to your hard drive.

If you happen to suffer a major issue and need to restore your entire system then Macrium Reflect gives you the option of creating a rescue USB stick or DVD. This will let you boot into a special version of Macrium Reflect where you can access your image backups and restore your hard drive. This will normally get you back to a bootable version of Windows with all your applications and files restored. If you find that Windows doesn't boot after you do the restore, then Macrium includes a utility that will recreate the Master Boot Record (MBR) and get you back up and running again.

Thanks to Roger Brown and Dennis Parsons for advice on the Linux section of this article. Some information about Mac OS backup options was sourced from Michael Podlabeniouk/Intuitive Strategy Computer Repairs.

Blocking Unwanted Emails

David Kretchmar, Computer Technician, Sun City Summerlin Computer Club

Sooner or later this happens to all of us. You continuously receive unwanted emails, (spam) from an individual or organization. Legitimate organizations usually have an Unsubscribe button within their message, which enables you to be dropped from their email list. If you attempt to unsubscribe from a less-than-legitimate mailer you are just confirming that your email address is good and even more spam will come your way.

Some individuals will not respect your request to stop sending (usually forwarding) you useless or offensive messages; more charitably they might lack the knowledge to be able to remove you from their mail distribution list.

Unwanted emails can be more than just bothersome or offensive. Some contain viruses that can render your system useless and destroy your data. Some people have had to abandon email addresses when they received many dozens of unwanted emails every day.

Fortunately, all email programs have a feature that will allow you to block all emails from specific email addresses.

I'm going to describe the email blocking procedures for three popular web-based email programs: **Yahoo Mail, Outlook, and Gmail**. If you are using another email provider, the described procedures can be used to at least point you in the right direction.

Each of these programs allows you to use a list of blocked senders for individual senders whose messages you don't want to receive but can't easily stop.

Yahoo Mail

Yahoo Mail can block all mail from up to 500 email addresses. All mail from these senders will be automatically deleted before you see it. To have Yahoo! Mail automatically delete all mail from a particular address:

- Left mouse click (hereafter I'll just say click if it's left) or just put your cursor on the settings gear in the upper right corner of the Yahoo Mail page.
- Click on “Mail Options” from the pull-down menu that has appeared.
- Click “Blocked Addresses” category under Advanced Options.
- Enter the unwanted email address under “Add an address:”.
- Click on “+”.

Your updated list of blocked senders will be saved automatically.

Outlook.com

- Click on the gear that appears in the upper right corner of the Outlook mail window.
- Click on “More mail setting”.
- Click on “Safe and blocked Senders”.
- Click on “Blocked senders”.
- Enter the unwanted email address in the “Blocked email address or domain” rectangle.
- Click on “Add to list>>”

Your updated list of blocked senders will be saved automatically.

Gmail

Ed: The following steps apply to the new MelbPC Google Workspace service.

- Click on the Settings gear that appears on the upper right corner of the Gmail window.
- Click on “Filters” near the top middle of the page.
- Click on “Create a new filter” at the bottom of the page.
- Enter the unwanted email address in the “From” rectangle.
- Click on “Create filter with this search>>”.
- Click on “Delete it”.
- Click on “Create Filter”.

Conclusions and Recommendations

Never reply to or unsubscribe from spam; it just alerts the sender that it has a good email address. When you get a spam message, click on your program’s “Spam” or “Send to Spam” or “Report as spam” to get rid of it and help your email provider learn to block messages from that server.

Even though email providers have active programs to help stop spam, it still comes. What winds up in your inbox is just a small fraction of the trash that is sent your way. Spammers are constantly changing techniques to defeat any filters.

You can work around the problem by creating and maintaining a “junk” or “throw down” email address that you know will be mostly spam. When I have to give out an email address to a website that I feel might be questionable, I provide the junk address and avoid possible spam in my “good” inboxes.

How an app to decrypt criminal messages was born ‘over a few beers’ with the FBI

David Tuffley, *Griffith University*

Australian and US law enforcement officials on Tuesday announced they’d sprung a trap three years in the making, catching major international crime figures using an encrypted app.

More than 200 underworld figures in Australia have been charged in what Australian Federal Police (AFP) say is their biggest-ever organised crime bust.

The operation, led by the US Federal Bureau of Investigations (FBI), spanned Australia and 17 other countries. In Australia alone, more than 4,000 police officers were involved.

At the heart of the sting, dubbed Operation Ironside, was a type of “trojan horse” malware called AN0M, which was secretly incorporated into a messaging app. After criminals used the encrypted app, police decrypted their messages, which included plots to kill, mass drug trafficking and gun distribution.

Millions of messages unscrambled

AFP Commissioner Reece Kershaw said the idea for AN0M emerged from informal discussions “over a few beers” between the AFP and FBI in 2018.

Platform developers had worked on the AN0M app, along with modified mobile devices, before law enforcement acquired it legally and adapted it for their use. The AFP say the developers weren’t aware of the intended use.

Once appropriated by law enforcement, AN0M was reportedly programmed with a secret “back door”, enabling them to access and decrypt messages in real time.

A “back door” is a software agent that circumvents normal access authentication. It allows remote access to private information in an application, without the “owner” of the information being aware.

So the users — in this case the crime figures — believed communication conducted via the app and smartphones was secure. Meanwhile, law enforcement could reportedly unscramble up to 25 million encrypted messages simultaneously.

But without this back door, strongly encrypted messages would be almost impossible to decrypt. That’s because decryption generally requires a computer to run through trillions of possibilities before hitting on the right code to unscramble a message. Only the most powerful computers can do this within a reasonable time frame.

Providers resist pressure for ‘back-door’ access

In the mainstream world of encrypted communication, the installation of “back-door” access by law enforcement has been strenuously resisted by app providers, including Facebook who owns WhatsApp.

In January 2020, Apple refused law enforcement’s request to unlock the Pensacola shooting suspect’s iPhone, following a deadly 2019 Florida attack which killed three people.

Apple, like Facebook, has long refused to allow back-door access, claiming it would undermine customer confidence. Such incidents highlight the struggle of balancing competing demands for user privacy with the imperative of preventing crime for the greater good.

Getting criminals to use AN0M

Once AN0M was developed and ready for use, law enforcement had to get it into the hands of criminal “underworld” figures.

To do so, undercover agents reportedly persuaded fugitive Australian drug trafficker Hakan Ayik to unwittingly champion the app to his associates. These associates were then be sold mobile devices pre-loaded with AN0M on the black market.

Purchase was only possible if referred through an existing user of the app, or by a distributor who could vouch for the potential customer as not working for law enforcement.

The AN0M-loaded mobiles — likely Android-powered smartphones — came with reduced functionality. They could do just three things: send and receive messages, make distorted voice calls and record videos — all of which was presumed to be encrypted by the users.

With time the AN0M phone increasingly became the device of choice for a significant number of criminal networks.

Building up a network picture

Since 2018, law enforcement agencies across 18 countries, including Australia, had been patiently listening to millions of conversations through their back-door control of the AN0M app.

Information was retrieved on all manner of illegal activities. This gradually enabled police to etch a detailed picture of various crime networks. Some of the footage and images retrieved have been cleared for public release.

One major challenge was for police to match overheard conversations with identities — as the AN0M phone could be purchased anonymously and paid for with Bitcoin (which allows secure transactions that can’t be traced). This may help explain why it took three years before police openly identified alleged perpetrators.

It’s likely the evidence obtained will be used in prosecutions now that a multitude of arrests have been made.

The future of encryption

Encryption technology is improving fast. It needs to — because computing power is also growing rapidly.

This means hackers are becoming increasingly capable of breaking encryption. Moreover, when quantum computers become available this problem will be further exacerbated, since they are massively more powerful than conventional computers today.

These developments will likely weaken the security of encrypted messaging apps used by law abiding people, including popular apps such as WhatsApp, LINE and Signal.

Strong encryption is an essential weapon in the cybersecurity arsenal and there are thousands of legitimate situations where it’s needed. It’s ironic then, that the technology intended by some to keep the public safe can also be leveraged by those with criminal intent.

Networks of organised crime have used these “legitmate” tools to conduct their business, secure in the knowledge that law enforcement can’t access their communications. Until AN0M, that is.

And while Operation Ironside may have sent a shiver through criminal subcultures operating around the world, these syndicates will likely develop their own countermeasures in this ongoing game of cat and mouse.

David Tuffley, Senior Lecturer in Applied Ethics & CyberSecurity, *Griffith University*

US lawmakers are taking a massive swipe at big tech. If it lands, the impact will be felt globally

Katharine Kemp, *UNSW*

Five antitrust laws proposed in the United States aim to aggressively rein in the market power of “big tech” companies and change the way they do business.

The set of bills, introduced on June 11, targets the enormous economic power wielded by the likes of Amazon, Apple, Facebook and Google (owned by parent company Alphabet).

The expansive proposals range from breaking up different businesses run by big tech, to more effectively preventing mergers known as “killer acquisitions”, in which big tech companies buy up rivals to stamp out threats to their market power.

The proposals would represent a massive change to US antitrust laws. US courts applying these laws currently tend to favour the growth of large companies and regard their economic power as a sign of superior economic efficiency.

Each of the bills has some support from both Democrats and Republicans. It’s remarkable the proposals have survived to this stage, in the face of record lobbying by big tech companies in Washington.

Even if only some of the proposals are passed as law, they will likely have significant consequences for the way big tech does business globally.

Who is targeted as “big tech” and why?

The five bills — collectively called “A Stronger Online Economy: Opportunity, Innovation and Choice” — would apply to any “covered platform” which:

- has at least 50 million active monthly users in the US
- has an owner with minimum net annual sales or market capitalisation of US$600 billion
- and is a critical trading partner for the supply of any product or service on or directly related to the platform.

This would capture at least Amazon, Apple, Facebook and Google. The proposals are the result of a 16-month investigation into these companies by the US House Judiciary Subcommittee on Antitrust.

The investigation famously saw the chief executives of Apple, Amazon, Facebook and Google each testify before members of the committee. This culminated in a 450-page report published by the majority Democrats in October last year.

The report slammed various strategies used by the companies as being monopolistic and harmful to innovation, competition and consumers. It said:

> To put it simply, companies that once were scrappy, underdog startups that challenged the status quo have become the kinds of monopolies we last saw in the era of oil barons and railroad tycoons.

How the proposals would change big tech

The measures included in the bills are extensive, but four key proposals stand out. First, big tech companies could be forced to split or sell certain businesses, in cases where running both the business and the platform creates a conflict of interest.

For example, Amazon has been accused of using data gained about third-party sellers in its marketplace, to gain a competitive advantage for its own Amazon Basics products.

Similarly, Apple might be stopped from selling its own products in competition with others in its app store or music store.

Second, platforms could be prevented from advantaging their own products over rivals' products on their platform, unless they could prove it wouldn't harm competition.

Google, for instance, has been accused of advantaging its services such as Google Shopping in search results. This kind of preferencing may prevent rival services getting a leg up, even if they offer a better service.

Third, the proposals target "killer acquisitions" made by big tech companies. These refer to cases where Amazon, Facebook, Apple and Google buy up smaller competitors.

These acquisitions may prevent better or more innovative products emerging. They remove a vital competitive threat, and venture capitalists may be discouraged from funding remaining rivals.

Consider WhatsApp, which began as a champion of privacy in instant messaging. Those privacy protections have been eroded since Facebook was allowed to buy WhatsApp in 2014.

Under one of the bills, big tech companies would face greater hurdles to achieve killer acquisitions. It would place the onus on the acquiring company to first prove it doesn't compete with the target company.

Finally, another proposal would require platforms to allow consumers to easily and securely transfer their digital history on a platform to themselves or to another platform. For instance, they could seamlessly transfer their Facebook history to another platform, and make the switch between platforms without losing their data.

How likely is it the proposals will become law?

Lobbyists for big tech are already hard at work in Washington, arguing such laws would weaken successful US companies, which would then be overtaken by rivals from China.

On the other hand, there are representatives from both major US political parties backing each of the bills, which could increase the chances of success.

However, this doesn't amount to a general consensus between the parties. Each tends to support measures against big tech for different reasons.

Many Republicans believe the platforms have a bias against their party and want to see more conservative-friendly rivals emerge. Democrats, meanwhile, focus on threats to democracy from the platforms' economic power and their ability to spread misinformation, including about public health and politics.

While it's unlikely all the proposals will ultimately become law, the strategy and support from both sides of politics means at least some changes will probably be legislated.

Splitting the measures into different bills also increases the chances some will be passed. If they were all included in one, a lack of support for one or two proposals could stop them all in their tracks.

Consequences in Australia and the world over

The effects of the proposed antitrust legislation will be felt well beyond the US.

Where measures are successfully imposed on a US company, it may decide to implement the same changes globally. For instance, Google last week announced it would make changes to its operations globally to comply with commitments Google made, following abuse of dominance complaints from the European Union (EU).

The EU has already been considering its own more stringent laws against large digital platforms. Lawmakers in other countries are likely to be influenced by these moves.

In Australia, the Australian Competition and Consumer Commission has had its Digital Platforms Inquiry extended into an ongoing five-year inquiry and is expected to make recommendations to government throughout this period.

Katharine Kemp, Senior Lecturer, Faculty of Law & Justice, UNSW, *UNSW*

Interesting Internet Finds

Steve Costello

The Two Types Of Cloud Data Threats And How You Protect Yourself

https://askleo.com/two-cloud-data-threats/

Leo Notenboom explains the two types of threats for having your data in the cloud and suggestions for protecting yourself from them. (Note: I have been using the cloud for years without any problems, but I only keep data that is recent and encrypted.)

How To Use Linux Live CD To Back Up Data From Windows PC

https://www.maketecheasier.com/rescue-your-pc-with-linux-live-cd/

If you use a Windows PC it is a matter of when not if you will have a problem being unable to access the PC. This article explains how to use a Linux Live CD to perform a rescue of your data.

Change Your Secret Router Password

https://cynmackley.com/2021/01/19/change-your-secret-router-password/

Something most people overlook for security is changing the router password. Cyn explains how to change this password, though the specifics vary depending upon the specific router.

Does Your IP Address Expose Your Home Address?

https://askbobrankin.com/does_your_ip_address_expose_your_home_address.html

I have heard this question asked at many user group meetings. This post from Bob Rankin gives the best answers I have seen so far.

What Linux Is And Why It Has Persisted?

https://www.askwoody.com/newsletter/free-edition-what-linux-is-and-why-it-has-persisted/

This article is from the free edition of the AskWoody newsletter. The article provides information about what Linux is and why it is still around and used. (Note: I subscribe to the paid edition, which contains mostly Windows-related articles.)

Why You Should Delete Emails Instead Of Archiving Them

https://www.howtogeek.com/709693/why-you-should-delete-emails-instead-of-archiving-them/

This is something I have not thought about until reading this. I have been using Gmail since 2005, so have many emails that are no longer necessary to have, and am working to clean them out to increase my storage capacity. I was surprised to have so much unnecessary stuff saved.

East SIG Report May 2021

Neil Muller

Host **Paul Woolard** opened the May meeting again via Zoom. This month he was seated with a small audience at Eley Road hall, our normal meeting place before the pandemic hit. This being the first hybrid meeting from Eley Hall, feedback from the audio system had to be solved before the meeting could commence. After a short delay **George Skarbek** presented his normal Q&A segment.

Q. Why do we have so much trouble doing these hybrid meetings?

A. Whenever you have more than the one microphone in the room, you can have feedback problems. I know all those involved are very competent people and eventually they'll sort it out.

Q. I'm having trouble with my Windows 10 machine. Win10 waas.medic.agent.exe is causing performance problems. When it starts up, it seems to be grabbing all the resources and nothing else will run. On start-up I can't even bring up Task Manager, even when nothing else is currently running.

A. Although I haven't heard of that problem, I've heard of similar problem where some rogue program grabs all the system resources. Because the problem is with a Windows application, that will make it a lot harder to resolve. It could have been a recent Windows update that has gone rogue. I suggest you do an update tonight as Microsoft may be aware of and have fixed the problem.

If you can't bring up Task Manager in the usual way from the task bar, there are two other ways you can try. I prefer pressing Ctrl + Shift + Escape (Esc) or alternatively Ctrl + Alt + Delete. You may then be able to get into Resource Manager.

[John Hall] I've just done a Google search and it appears was medic.agent.exe has something to do with Windows Updates. I suggest going into Window Updates and turn off all updates. To do this, say that you're on a metered connection and you don't want Windows updates to start. Turn your computer off and reboot and all updates should stop.

Q. Does anyone know of a program that will sync a Windows PC with an Android tablet? I don't want to sync the whole tablet, just Word documents. I'd like to be able to sync when the program recognises, I'm on a certain wi-fi connection.

A. I don't know of a program that will do that, but if you connect between the devices with a cable, you will then be able to copy from one to the other.

[John Hall] Google Drive or Microsoft OneDrive could be used to store your Word documents and access them from either device.

Q. I have a relative's laptop that boots up with a display, System Interrupt 100% in use, a few seconds later the CPU shuts down and a display shows the hard drive at 100% use. At that time the machine is unusable. I've run anti-virus and I'm current running sfc (system file checker) to see if there's any problem there. Has anyone got any suggestions as the relative is leaving for overseas soon?

A. Almost certainly it's not a virus. Viruses try to be invisible while doing their nasty work before they are noticed and you try to kill them. If you can start Task Manager that will tell you what program is taking up all of the CPU or hard disk.

There are many programs that can cause system interrupts. Therefore, system interrupt isn't much of a clue. I would go to the Event Viewer and have a look there. You will need to look either under Application or

System. Have a look at the time when things went to 100% and that may give you a clue what the culprit is. I'd say you've got a 30% chance there of tracking it down. You'll have to press Ctrl + Shift + Esc or Ctrl + Alt + Del to stop the process and get into Task manager. Once you find what program is causing the problem, stop it. You can then uninstall it or stop it from starting.

[Questioner] The file that is causing the hard drive to run at 100% seems to be a different program each time the computer starts.

[Audience member] To speed up hard disk performance (to overcome slow operation) enable write caching in Windows 10. This unfortunately increases the risk of data loss in case of power failure.
How to: Open Device Manager □ Disc Drives □ Double-click the particular Disk □ Properties □ Policies □ Enable write caching. If this doesn't do anything significant, try Opening Administrator Command Prompt and CHKDSK the disk.

[Audience member] I have a hard disk that is showing 100% disk use, but no programs are running. I did a Windows Check Disk (Chkdsk.exe) and found numerous bad sectors which Windows was trying to correct, thus causing the 100% usage. I'm currently trying to get all my data off this drive before the hard drive fails completely.

[Update from Questioner] As a result of the above problem, and the fact that an external keyboard is mandatory because 8 keyboard keys are unusable, a new laptop was purchased so the problem has not been solved.

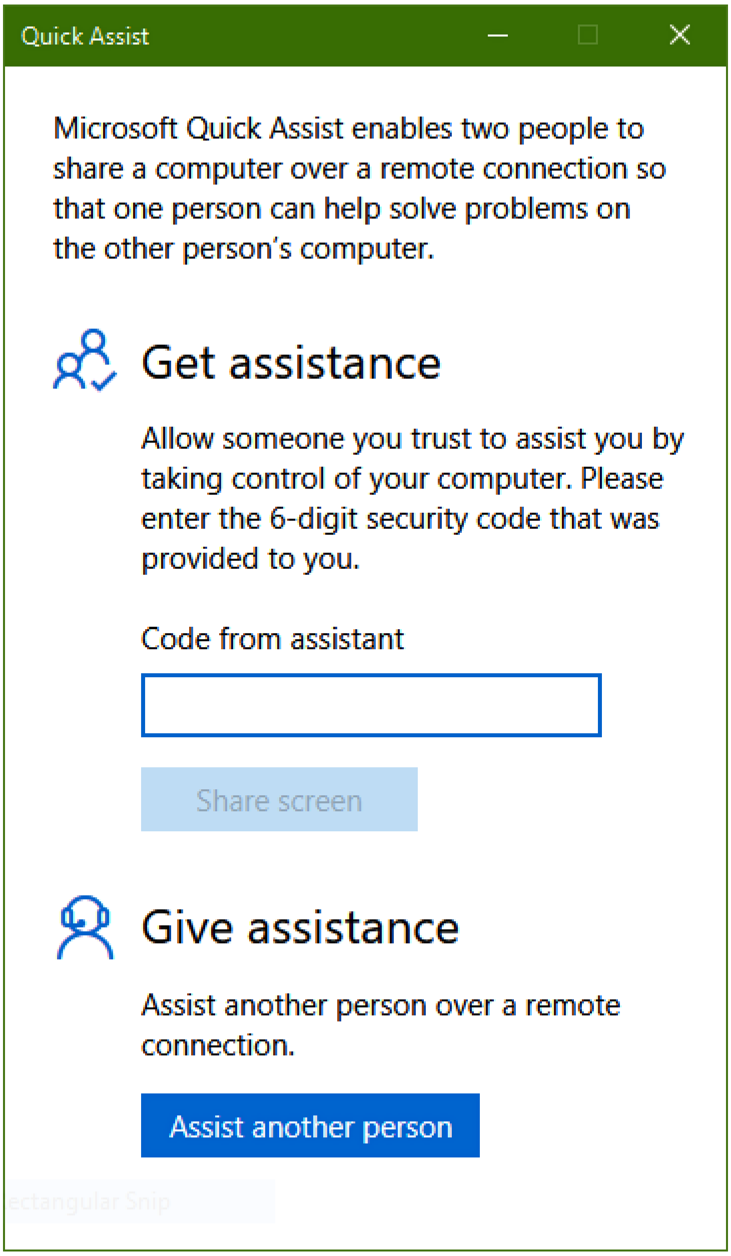
Q. I put my laptop into sleep mode when I've finished using it, so that I don't have to wait while it boots the next time it's used. At night I close the lid, to put Windows into sleep mode, so it's ready for the next use. I use sleep mode with my desk top computer without any problems, but my laptop keeps humming and is burning hot to touch in the morning. This is a gaming laptop so could that be the cause?

A. Again you will need to go into Task Manager to find how long it goes to sleep for and how deep the sleep is. Under power settings check whether the display goes off, the hard drive stops etc.. Because the laptop is so hot in the morning, something must be running while it is asleep. I suggest before you put it to sleep, open Task Manager and go to the tab that shows CPU and disk usage. When you wake the laptop up from its sleep, as Task Manager is still running you will be able to find what has been running while it's asleep. You will then see what has been chewing up vast amounts of resources and causing the heat.
[Audience member] There used to be an old setting in Windows that would continually wake up Windows from sleep.
[George] That was called Wake on LAN and is used to wake a computer on a network when other family members want to use files on that computer. You can switch that off if it's on. However, that wouldn't cause the computer to run so hot.

Last month **Dave Botherway** gave a presentation on Zoom's "Remote Control" feature. This month he presents the Microsoft equivalent called "Quick Assist". Quick Assist has been available since Windows 8, but is still relatively unknown, namely due to the popularity of other sharing programs such as Team Viewer. Quick Assist is now used by MelbPC's iHelp team after TeamViewer required MelbPC to take out a commercial licence.

Quick Assist allows 2 Windows 10 computers with a Microsoft account, to connect to one another on the internet. A person at one of the computers can then control the other to solve and fix any problems without the need to be sitting in front of the faulty computer. Both computers need to be turned on and the person needing assistance has to give approval before control is given to the other person. The person at the faulty computer can take back control at any time if concerned at what is happening.

Dave suggested the easiest way to find Quick Assist is to use the Windows Search button on the taskbar. After the first 3 letters had been entered in the search bar, Quick Assist appeared at the top of the list of search items. From the list click on Quick Assist and the "Quick Assist" window shown in Figure 1 appears.



Microsoft Quick Assist enables two people to share a computer over a remote connection so that one person can help solve problems on the other person's computer.

Get assistance

Allow someone you trust to assist you by taking control of your computer. Please enter the 6-digit security code that was provided to you.

Code from assistant

Give assistance

Assist another person over a remote connection.

Figure 1 – Quick Assist Window

In the Quick Assist window two options are available, to “Get Assistance” from a remote person or to “Give Assistance” to another person.

Dave first demonstrated how to “Get Assistance” from a remote user, followed by the reverse process where he selected “Give Assistance” to another user. As both techniques are similar, only the more common option of giving assistance to a remote user will be shown in this report.

To give assistance both computers have to be on, running Windows 10 and have a Microsoft account. Quick Assist will not connect to a remote computer without someone sitting in front of that computer. This is necessary as the remote user needs to approve the connection before the helper can take control of the remote computer.

Select “Quick Assist” as outline earlier and select the “Assist another person” button. You’ll next be asked to enter your Microsoft account details. Once done “Quick Assist” generates a 6-digit security code that you need to give to the remote user you are helping.

The 6-digit code can be sent by mobile phone (voice or text) or by email to the remote user you are assisting. The security code generated only lasts 10 minutes before it expires and a new code is needed. The 10-minute limit does not apply once the connection is made.

In the window below the 6-digit security code, select the type of help that will be given. Here Dave selected “Provide instruction”. Once selected the Window refreshes and you select “I provide instructions”. A new window then opens where you have the option to “Take full control” or View screen”. Dave selected “Take full control” and then clicked the “Continue” button. Dave then waits for the remote user to grant permission. While waiting the helper sees a message “Waiting for the sharer to grant permission”. This process and those that follow, is outlined in the flow chart at the end of this report.

At the remote computer the user needs to opens “Quick Assist” and add their Microsoft account details before they can proceed. (Figure 1). When these details are confirmed, the 6-digit code under “Get assistance” is entered. Once the last digit is entered the “Share screen” button turns blue (becomes active) and is selected. The remote user will then see the message “Waiting for helper to set up this session”. After a short period, you see a new window titled “Share your screen”. This is where you give your permission for the helper to “Take full control” of your computer by selecting the “Allow” button.

After a short period, the remote computer is connected to the helper and displays a small toolbar at the top of the screen to indicate screen sharing is on. (Figure 2). The remote user can pause control of sharing by selecting the pause icon on this toolbar.

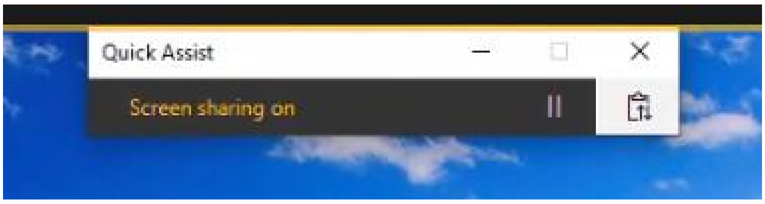


Figure 2 – Remote computer “Screen sharing on” toolbar

When the connection is complete, Dave can see the remote computer’s screen as if he was sitting in front of it. He is then able to control the remote computer with his mouse and keyboard. At the top of Dave’s screen is a toolbar showing icons that may be used to assist in diagnosing any problems. (Figure 3). After opening programs and adjusting the time on the remote computer, Dave selected “End” from the toolbar, to close Quick Assist and stop sharing.

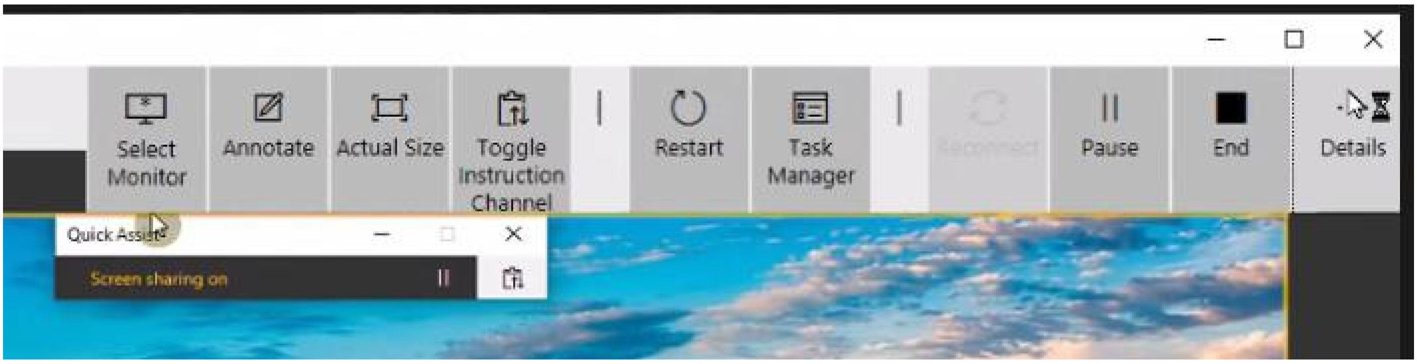
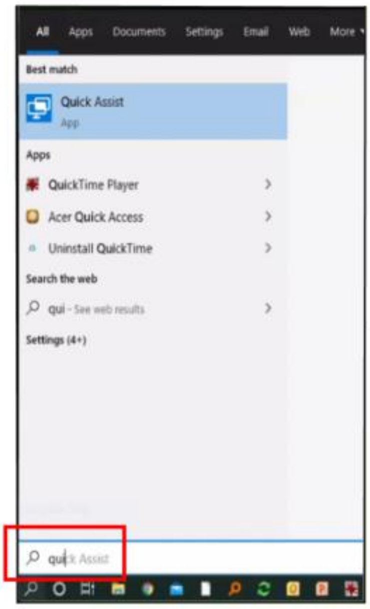
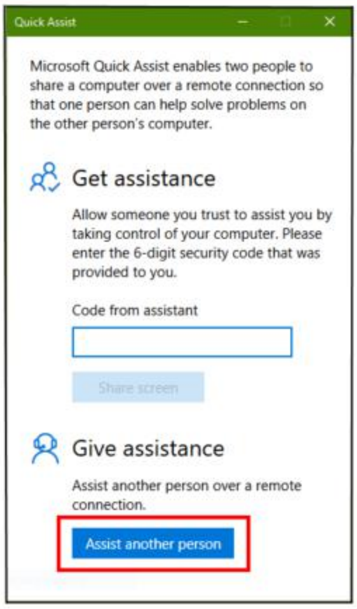


Figure 3 – Quick Assist toolbar displayed on the helper’s computer

The following flow chart shows the various “Quick Assist” windows, in chronological order, that a helper and the remote user see when giving assistance to a remote user.

Computer Giving Assistance





Microsoft Quick Assist enables two people to share a computer over a remote connection so that one person can help solve problems on the other person's computer.

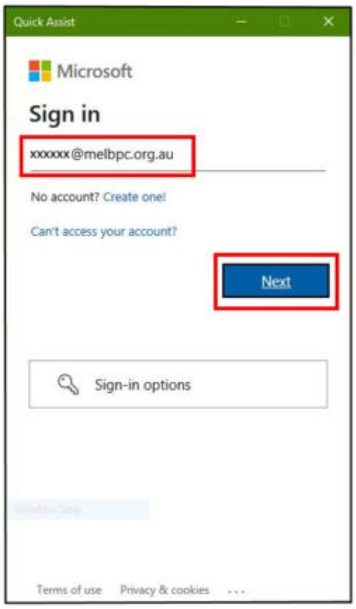
Get assistance

Allow someone you trust to assist you by taking control of your computer. Please enter the 6-digit security code that was provided to you.

Code from assistant

Give assistance

Assist another person over a remote connection.

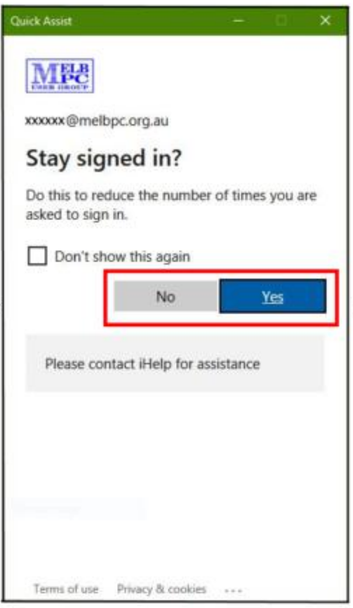


Sign in

xxxxxx@melbpc.org.au

No account? Create one!

Can't access your account?



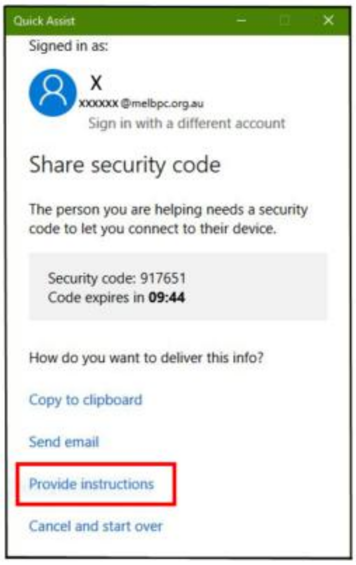
xxxxxx@melbpc.org.au

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again

Please contact iHelp for assistance



Signed in as:

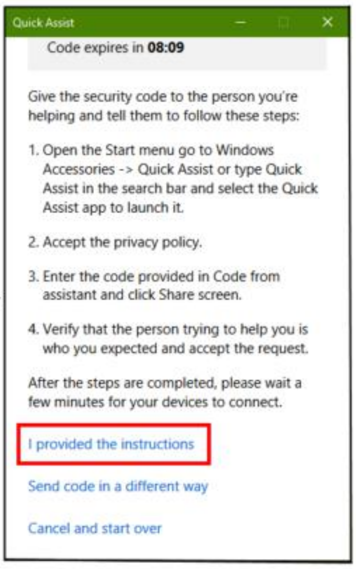
X
xxxxxx @melbpc.org.au
Sign in with a different account

Share security code

The person you are helping needs a security code to let you connect to their device.

Security code: 917651
Code expires in **09:44**

How do you want to deliver this info?



Code expires in **08:09**

Give the security code to the person you're helping and tell them to follow these steps:

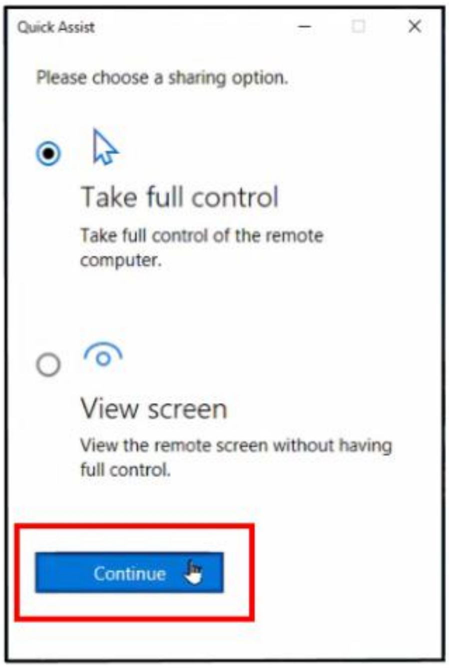
1. Open the Start menu go to Windows Accessories -> Quick Assist or type Quick Assist in the search bar and select the Quick Assist app to launch it.

2. Accept the privacy policy.

3. Enter the code provided in Code from assistant and click Share screen.

4. Verify that the person trying to help you is who you expected and accept the request.

After the steps are completed, please wait a few minutes for your devices to connect.



Quick Assist

Please choose a sharing option.

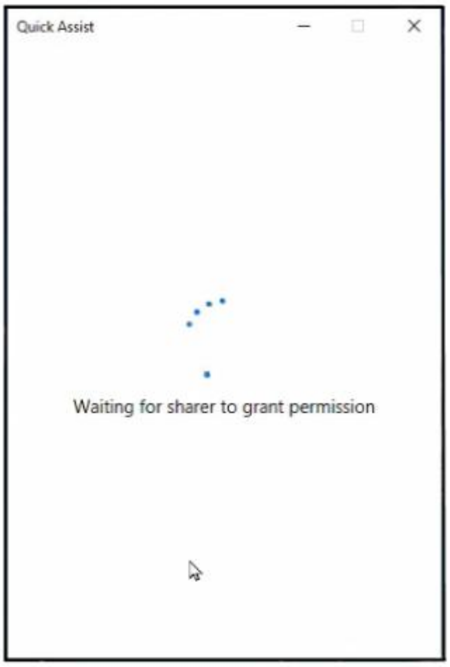
● Take full control

Take full control of the remote computer.

○ View screen

View the remote screen without having full control.

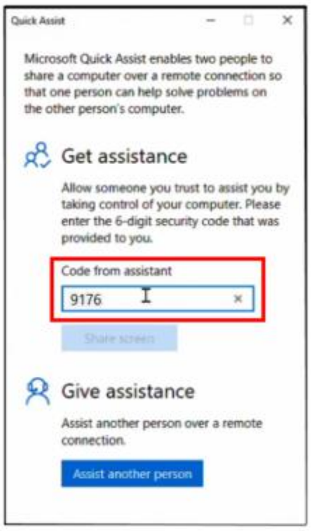
Continue



Quick Assist

Waiting for sharer to grant permission

Remote Computer



Quick Assist

Microsoft Quick Assist enables two people to share a computer over a remote connection so that one person can help solve problems on the other person's computer.

Get assistance

Allow someone you trust to assist you by taking control of your computer. Please enter the 6-digit security code that was provided to you.

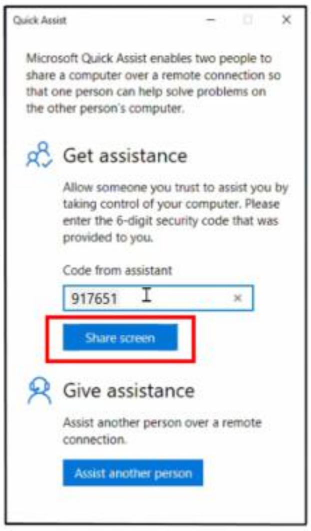
Code from assistant: 9176

Share screen

Give assistance

Assist another person over a remote connection.

Assist another person



Quick Assist

Microsoft Quick Assist enables two people to share a computer over a remote connection so that one person can help solve problems on the other person's computer.

Get assistance

Allow someone you trust to assist you by taking control of your computer. Please enter the 6-digit security code that was provided to you.

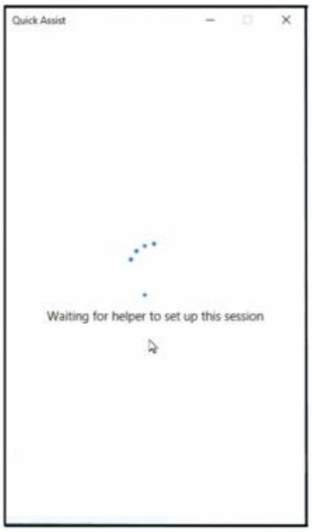
Code from assistant: 917651

Share screen

Give assistance

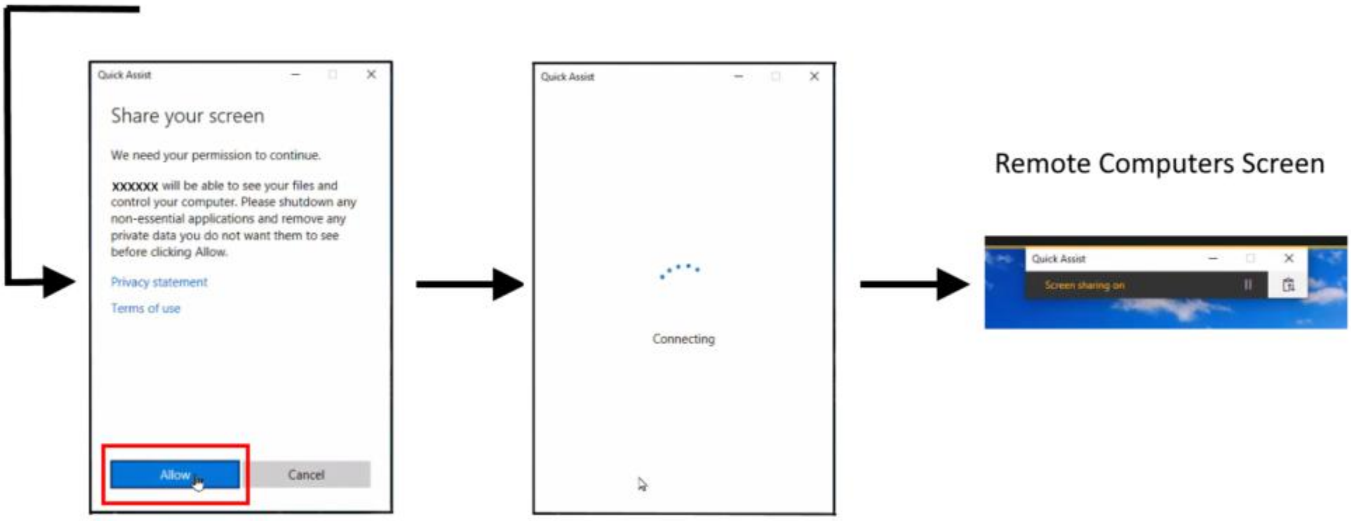
Assist another person over a remote connection.

Assist another person



Quick Assist

Waiting for helper to set up this session



Quick Assist

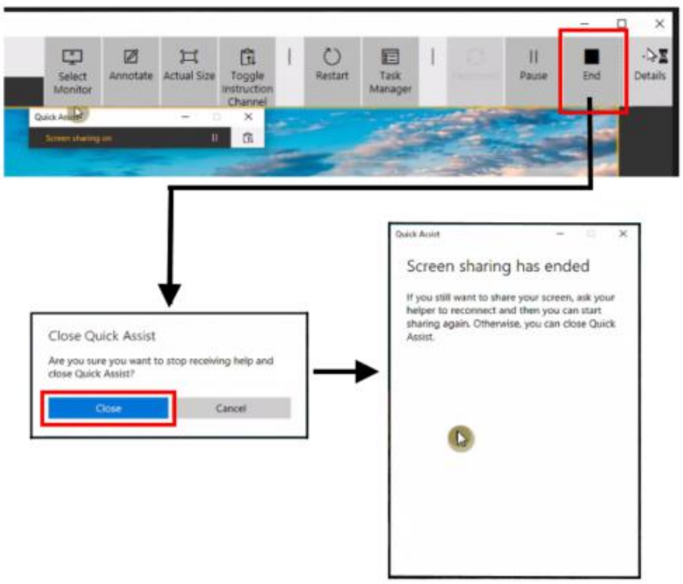
Share your screen

We need your permission to continue.

xxxxxx will be able to see your files and control your computer. Please shutdown any non-essential applications and remove any private data you do not want them to see before clicking Allow.

Remote Computers Screen

Computer Giving Assistance



Close Quick Assist

Are you sure you want to stop receiving help and close Quick Assist?

Screen sharing has ended

If you still want to share your screen, ask your helper to reconnect and then you can start sharing again. Otherwise, you can close Quick Assist.

Questions followed and the meeting concluded with informal discussions between audience members related to using Quick Assist.

DOTW Winners May 2021

Roger Brown

DOTW is a lighthearted look at some of the sillier events of the week. Don’t take it too seriously and do pop over to Chit Chat and vote each week. Thanks to those of our members who occasionally ‘feature’ for taking the gentle humour in such good part.

May was a month where members of the Chit Chat group very deeply felt the loss of our member and group founder Judy Bednar. We continue DOTW in her memory.

May winners were:

• Queensland police who when contacted by a caller seeking immediate protection from domestic violence took an hour to respond and when they did and received no answer simply wandered off taking no action to ascertain whether the caller was still alive. She wasn’t – she’d been murdered!!

• The hairdresser in south-west Victoria who says she won’t accept customers who have been vaccinated against COVID-19 because in her view they may infect other clients (a view deemed nonsense by medical experts).

• Our very own Kevin Martin for one of the worst bad jokes ever posted on Yammer.

• Aged Care Services Minister Richard Colbeck for constantly demonstrating almost complete ignorance of the vaccination rollout to to the aged care centres for which he is responsible.

Thanks to all participants, including those who feature in our supplementary LOSER award!!

Yammer Highlights May 2021

Dennis Parsons

In Memory of Judy Bednar

We had a terrible shock when we heard that a long-time member, Judy Bednar, had been murdered in her home and her son subsequently arrested. She was well known to many members through her active participation in the original Melb PC newsgroups and then Yammer, with many of us considering her a friend. As ever with the newsgroups and Yammer the discussions she was involved in ranged far and wide, from computer related "why is it so?" to her experiences in communist Hungary and when she came to Australia in the late fifties, her feelings about Israel, and sadly the decades of problems she had with her schizophrenic son.

A number of us had met her personally and visited her home to help her with solving computer related problems, along with the occasional handyman chore while we were there. Consequently, we were referred to as her "Clayton's husbands" and she often sought help in working out how to achieve some household task or repair.

Judy enjoyed gadgets, she loved her coffee machines, TVs, PVRs and computers but was plagued by what we came to know as the Bednar Poltergeist, a mysterious force that loved to torment her by altering settings and stopping technological devices working properly. Of course, said poltergeist vanished more often than not when a visit was paid only to reappear shortly after.

Such a sad and horrible end to a long life. Rest in peace Judy.

<https://www.yammer.com/melbpc.org.au/#/Threads/show?threadId=1212247412891648>

We're taking a collection in memory of Judy and making a group donation to Domestic Violence Victoria (DV Vic) and the Domestic Violence Resource Centre Victoria (DVRCV). If you'd like to contribute you can either make a direct bank deposit, or phone the office during normal business hours and pay by credit card. Direct deposit is preferred. Please refer to the following link for details and note collection closes on June 29th.

<https://www.yammer.com/melbpc.org.au/#/Threads/show?threadId=1228318139604992>

Computer Help

Now that the official Service Victoria QR code is the only type that can be used to check in when you visit businesses and other venues members have raised a few issues. Mostly it’s been working okay but a few people have been caught out by older phones as the app requires Android 6.0 or later, and as the QR code is quite dense some cameras, particularly on older phones, struggle to read them.

One member lamented the lack of support for older phones, particularly as many older people use phones handed on by grandchildren, but for better or worse technology moves on and only around 4% of phones run less than Android 6.0. Older Android versions don’t support the features required so simply aren’t suitable for use with the app, even if it could be installed.

There are phones available that can run Android 11, the latest version, for under $130 and if that’s too rich slightly older models can be bought for under $50, just be aware they’re probably locked into one of the phone companies and most likely can’t be updated to newer versions of Android. Regardless, a data enabled phone account is required.

Or of course you can still check in using pen and paper.

<https://www.yammer.com/melbpc.org.au/#/Threads/show?threadId=1235600943153152>

Security, Scams and Phishing

Graham reported he’d received an e-mail sent using the address of another member and containing a link to an “invoice” – clearly a phishing e-mail. On the surface we thought it was just a case of a spoofed e-mail, but other members reported receiving it too and anti-spam measures on the Microsoft servers reported to our mail admin that they were blocking the member from sending.

So rather than being a spoofed e-mail it was likely the member had an infected system that was sending the e-mails. Harry reported that the iHelp team was actively engaged in helping the affected member. Hopefully, a few phishing e-mails were the only damage.

<https://www.yammer.com/melbpc.org.au/#/Threads/show?threadId=1237375757574144>

<https://www.yammer.com/melbpc.org.au/#/Threads/show?threadId=1237972729569280>