



[S C C C](#)

Buderim Meeting Friday 31.10.2025

Halloween

Time - 12 pm to 3 pm

100 Buderim Pines Drive, Goodlife Centre Buderim

Admission - \$4

Nevil Eyre Android Phones & Tablets & Home automation

Tutorial Room Bill Maxwell

Three Laptop computers set up to answer questions: Windows /
Linux / Mac-book Air

1. Q&A
2. Stop using Passwords - Use a Passkey - What is a Passkey?
3. How to set up a passkey on your Google Account.

Discussion on iPad and iPhone functions.
Limited help with basic Apple Mac computers.

Sat. 1.11.2025

8.30 to 11.30 am

Meridan Plains

70 Springs Dr. QLD 4551

[here](#)

Hands on Help - Windows, Linux and Chromebooks

Please wear your Name Tag.

General Security Tips

1 Avoid downloading files from unknown or untrustworthy sources to avoid potential malware on your device.

2 Do not connect unknown USBs or other devices to your computer.

3 Depending on your email provider, you can set up spam filters to protect against phishing threats and avoid malware that's attached to emails.

4 It's important to run a malware scan to ensure there is no presence of dangerous malware on your computer.

To do this, navigate to Settings > Privacy & Security > Windows Security > Virus & threat protection.

The majority of these processes should automatically run in the background, but you can check them here.

5 In Virus & threat protection, you can click on Scan options to run different types of scans on your device.

Quick scan is recommended for your usual scheduled scans and will look at the locations where malware

could be hidden that could affect starting your device.

A full scan takes much longer but performs a deep scan of your device including archived files, network drives, and more.

6 To ensure your device is protected at all times, toggle Real-time protection on in the Virus & threat protection settings menu.

This will locate any malware on your device and stop it from installing.

7 Your device should automatically download the latest security intelligence to keep your device protected.

However, you can manually check for updates by going to Virus & protection settings > Protection updates.

8 In addition to virus protection, you can also enable ransomware protection on your device in the Virus & protection settings > Ransomware protection menu. Toggle on to allow controlled folder access.

9 If an item that you know is 100% safe gets flagged by Windows Defender as a threat, you can allow some threats through.

You can do this via Virus & protection settings > Allowed threats.

10 Since Windows Defender comes as part of Windows 11, there is no need to install any third-party anti-virus software.

If you do install third-party software, it could cause conflicts and cause Windows Defender to stop working, which is **counterproductive**.

Fast Startup

Most people don't actually ever need to [access their BIOS/UEFI setup menu](#).

However, if you do ever need to access this setup menu, it'll be a lot harder to do so with Fast Startup activated.

After all, your window of opportunity to enter the BIOS/UEFI setup menu is during the part when your PC is booting up.

Windows Fast Startup makes that booting process much shorter, meaning your window of opportunity to access

your BIOS/UEFI menu is greatly reduced. It's not impossible to make it, but it is really annoying if you want to access

that menu with any regularity. Of course, if you know you need to access it at a certain point, you could always just turn

Fast Startup off real quick before turning it back on again later.

In general, it is a lot more convenient to access the UEFI/BIOS by Shift-clicking the Restart button from within

Windows if you have Fast Startup enabled.

So far, it may sound like there is no reason to ever leave Fast Startup on, especially if it can cause you

such a wide array of problems. But it's not like it's all bad. If you have this feature on and your PC

doesn't seem to be having any trouble because of it, then by all means, leave Fast Startup on.

It can even be beneficial for older computers that are still using mechanical hard drives.

With those types of devices, Fast Startup really can make a big impact on boot times.

That said, if you're using any device with an SSD, Fast Startup really isn't doing that much for you,

even if it isn't causing any problems. SSDs are already so fast, that Fast Startup will likely, at best,

only give you a second or two of increased boot speed, and is it really worth the risk of the feature causing trouble when it's not that helpful for you anyway?

If you agree with that assessment, disabling Fast Startup is pretty easy.

There are only a few steps you need to take to turn it off. It may vary whether you are using Windows 11 or Windows 10.

Below is the quick process required to turn this feature off in Windows 1

How to Disable Windows Fast Startup

This process should only take you a minute at most.

First, open the Control Panel, and select "Hardware and Sound."

Then under Power Options, you should select "Choose what the power buttons do."

Finally, select "change settings that are currently unavailable."

You will then be able to enable or disable the "Turn on Fast Startup" option.

Large Language Models can get “Brain Rot”

We propose and test the LLM Brain Rot Hypothesis: continual exposure to junk web text induces lasting cognitive decline in **large language models** (LLMs).

To causally isolate data quality, we run controlled experiments on real Twitter/X corpora, constructing junk and reversely controlled datasets via two orthogonal operationalizations: M1 (engagement degree) and M2 (semantic quality), with matched token scale and training operations across conditions. Contrary to the control group, continual pre-training of 4 LLMs on the junk dataset causes non-trivial declines (Hedges' $g > 0.3$) on reasoning, long-context understanding, safety, and inflating "dark traits" (e.g., psychopathy, narcissism).

The gradual mixtures of

junk and control datasets also yield dose-response cognition decay:

for example,

under M1, ARC-Challenge with Chain Of Thoughts drops 74.9 -> 57.2 and RULER-CWE 84.4 -> 52.3 as junk ratio rises from 0% to 100%.

I find myself doom scrolling Instagram reels or Youtube shorts from time to time.
But apparently, LLMs can literally rot their own brains the same way.

Data scientists fed models months of viral,
short but high-engagement posts and watched cognition collapse:

- Reasoning fell by 23%
- Long-context memory dropped 30%
- Personality tests showed spikes in narcissism and psychopathy

And even after re-training on clean, high-quality data,
the damage was already dealt and representational “**rot**” **persisted**.

Regularly Back Up Data for Peace of Mind

Aussies are being warned about a [new email scam](#) doing the rounds, which claims to be sent by an online security software company.

If you feel you have fallen for a scam, contact IDCARE, a free government-funded service which will work with you to develop a specific response plan to your situation, and support you through the process.

<https://www.idcare.org/>

1. Phishing Emails: In a phishing scam, the attacker will send their target a message claiming to be an official, trusted party.

This kind of urgent communication works well in pressuring the recipient to comply with the senders request.

2. Remote Desktop Protocol. Simple: **Don’t allow Remote Connections.**

3. Flash Drives. **Don’t allow strange Flash Drives to be used on your PC..**

Disclaimer: Although articles in this newsletter are checked for content, no warranty can be given for any loss

resulting from the use of material in the newsletter.

Articles and advertisements are printed in good faith and views and opinions are not necessarily those held by SCCC Inc.