



S C C C

Buderim Meeting Friday 21.11.2025

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 Microsoft Spying on you. New free program to turn off Windows spying tools. O&O Shutup 10++
3. New Chrome Features.
4. Replacement for BOM Radar - [Rain Rate](#)

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

Sat. 22.11.2025

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.

Christmas / New year break information 2025 / 2026

Last meeting Buderim 12 December 2025

First meeting Buderim 16 January 2026 at Goodlife Centre

Last meeting [Meridan Community Centre](#) 13 December 2025

First meeting 17 January 2026 at [Meridan Community Centre](#)

How to Kill a Process on Mac

To find and kill a process that's causing an issue in macOS is to launch Activity Monitor.

You can [do this using Spotlight](#) (hit Command+Spacebar then start typing "activity" and hit Enter

when you see the app) or by finding and launching the app under the Applications > Utilities folder.

Activity Monitor has several [views you can use to isolate problems](#).

On the CPU tab, you can see which apps are using the most processing power right now (sort by the "% CPU"

tab to see the hungriest processes. You can also use "Memory" to sort by RAM usage,

“Energy” to find [which apps are using the most power](#), “Disk” to sort by disk usage, and “Network” to sort by data sent and received.

On top of this, you can use the “Search” box in the top-right corner to search for a process name.

You can find the core process and associated processes this way, for example searching for Safari

will find the core app, networking processes, individual tabs, extensions, and more.

Find the process you would like to kill and then click on the “X” button in the top-right left corner of the screen.

You can then choose between “Quit” and “Force Quit” to attempt to send a quit command (to give the process time to save your data)

or a force quit command (to kill the process immediately, ideal if it’s crashed).

Find out more about [identifying processes that are safe to kill on your Mac](#).

If the process you want to quit is an app in your dock, you can [force close it](#) which should kill it even if it has

crashed and become unresponsive. To do this, find the app in your dock and [right-click](#) (or control-click) then

hold the “Option” key on your keyboard and choose “Force Quit” at the bottom of the list.

You can force quit anything, whether it has crashed or not, but you’re more likely to lose unsaved progress by doing so.

If you find that you frequently need to do this, learn [how to troubleshoot crashing apps on your Mac](#).

Switch to passkeys when available

Not all 2FAs are made equal, and so better additional factors have been developed to combat things like SIM-swap fraud.

Passkeys are a great solution, because they make use of an on-device encryption key that requires physical possession of that specific device.

If you have the option to use passkeys, I recommend it, but then you need to have good security for that device.

Consider using a passcode or password instead of biometrics, for example.

Keep your devices and software up to date

Hackers use vulnerabilities discovered in hardware and software to gain access to information or to bypass security.

When these exploits become known, the holes are usually patched before or soon after.

This doesn't mean much if your device doesn't have the latest security updates, and it's a key reason you shouldn't use devices that are no longer receiving security updates.

Watch for phishing and social engineering tricks

This is done through spoofed emails or text messages with links to fake websites.

Social engineering is broader, and includes phishing, but also includes all the methods of getting compliance from a human being.

Like phoning you and pretending to be your boss or a representative of your bank.

Use a secure recovery setup

The worst situation happens when someone gets access to your accounts and then **locks you out of that account.**

This often happens with social media accounts, for example. Here the intruder may then change the associated email account or otherwise prevent recovery.

So if a service offers recovery or backup methods, be sure to set them up as soon as possible.

Store them somewhere safe and offline, such as on paper in a safe.

This way, if the worst does happen, you can provide absolute proof you are the rightful account owner.

Regularly review and clean up your accounts

If you're using a password manager or something like Google Chrome's security checkup,

you can see if your passwords have been in a data breach.

Take it seriously if accounts come up in those lists.

Delete accounts that you don't use anymore, and change compromised passwords in each service.

Periodic reviews are important, and you should change your most important account passwords

every few months whether they've been listed in a breach or not.

After all, those breaches are just the ones we know about!

From Peter,

Window's future as an AI controlled agentic operating system.

It seems that a large number of users don't like that idea.

Agentic system = Unlike traditional AI models, which operate within predefined constraints

and require human intervention, agentic AI exhibits autonomy, goal-driven behavior and adaptability.

The term “agentic” refers to these models’ agency, or, their capacity **to act independently and purposefully**.

"Agentic" describes something or someone that is capable of acting independently, making decisions,

and achieving outcomes on their own. In the context of AI, an agentic system uses AI agents to perform tasks with a degree of autonomy, like reasoning, planning, and taking action without constant human oversight.

This is in contrast to traditional systems that simply follow pre-programmed instructions. "

Artificial Intelligence needs lots of Power.

More wind mills and Solar panel fields

- AI models such as ChatGPT “are just insatiable in terms of their thirst” for electricity.

- “The more information they gather, the smarter they are, but the more information
- they gather to get smarter, the more power it takes.”
- Without greater efficiency, “by the end of the decade,
- AI data centres could consume as much as 20% to 25% of US power requirements.
- Today that’s probably 4% or less ... That’s hardly very sustainable, to be honest with you.”
- The article also noted that the International Energy Agency said a request to ChatGPT
- requires 2.9 watt-hours of electricity on average – equivalent to turning on a 60-watt light bulb for
- just under three minutes or almost 10 times as much as the average Google search.

1. Pause, don't tap

If it's unexpected or urgent, slow down... no quick-pay links, open your bank or service app directly instead.

2. Ring a caller back on a verified number

If money or data is involved, do not provide this on an incoming call, ring the company on the number on their website or your card, not the one in the message.

3. Assume anyone can be fooled

Treat every email as suspicious. Use strong logins like passkeys, and keep less personal info public (private Facebook profiles) so scammers have less to mimic.

Regularly Back Up Data for Peace of Mind

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.