



S C C C

Buderim Meeting Friday 7.11.2025

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. New Start Menu for Windows 11.
3. A review of all the different types of Video Connectors
4. What are all those connectors on the back of PD for?

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

Sat. 8.11.2025

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.

Hot on the heels of a [Chrome emergency security update](#) issued by Google, Microsoft has now also confirmed an emergency

fix for a critical Windows vulnerability. Acting immediately is paramount, as the Cybersecurity and Infrastructure Security Agency

has warned that attacks are already underway and issued a binding directive requiring federal agencies to update now.

Earlier this year, I reported on a data leak that included a whopping [184,162,718 passwords and logins](#) impacting the likes of Apple,

Facebook and Instagram users. That data leak was disclosed on May 22, and now, in a rather spooky seeming coincidence,

news of 183 million passwords and login credentials from an April 2025 breach has emerged.

Adding the details of website URLs, email addresses and passwords to the Have I Been Pwned database, owner Troy Hunt said

the data consisted of both “stealer logs and credential stuffing lists” including confirmed [Gmail login credentials](#).

Gmail users have been warned of a surge in [image-based attacks](#), TikTok users are facing a [VIP upgrade offer threat](#),

and Lastpass has urged users not to change their master passwords as a [you’ve been hacked](#) email circulates.

Now, security experts at KnowBe4 have issued a warning for PayPal users as cybercriminals use a genuine

PayPal email address to send an invoice. Paypal itself has responded to this attack with a ‘**do not pay, do not phone**’ warning.

Here’s everything you need to know about the latest scam that could prove costly if you don’t follow the advice given.

This may well sound familiar, not least as this type of [TOAD attack](#) is something I have detailed before.

A Telephone-Oriented Attack Delivery threat usually contains a PDF invoice or other seemingly official document,

along with messaging that uses urgency and fear of financial loss to persuade victims to call an **adversary-controlled** phone number.

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](#)

I genuinely believe most people who still use **Outlook never chose to. It came with Windows**, or they assumed their [@outlook.com](#) address

would work best with the Outlook client (it doesn't), or they're already paying for a Microsoft 365 subscription.

But none of these are good reasons to stay trapped in a bad app.

The Outlook problem is a complete trilogy of failure: the service (Outlook.com), the client (Outlook), and the company

behind both (Microsoft). None of them stand up to the competition.

I ditched Outlook a while ago and switched to web clients for a while — that's how much I disliked using it. Eventually, I found better desktop options.

If you're on Android, just use Gmail. It's faster and more stable. If you're on Apple devices, use Apple Mail. It's native, clean, and efficient.

And if you're on Windows like me, don't worry. You have options.

Thunderbird, from Mozilla, is free, open-source, and highly reliable. If you prefer something more modern-looking, try Mailspring —

it's also free, open-source, and visually polished. I settled on Mailspring after a year of frustration, and it's been the best email experience I've had on Windows.

Outlook's email service is infamous for its paranoia. I've lost count of how many times I've had to re-enter my password or verify

with two-factor authentication just to sync my inbox. Supposedly, it's for security.

But I have accounts from four other providers in the same client, and none of them harass me this much.

And that's just the beginning. I once lost an important Outlook inbox entirely due to Microsoft's overzealous security system and its nonexistent customer support.

Take this as a warning: if you ever get locked out of your account, you're on your own. You'll spend hours trying to reach a human

through AI chatbots, and if you finally get through, the agent will be useless. **You'll lose access forever.** I did. And I'm still bitter about it.

Outlook feels like a microcosm of everything wrong with Microsoft today. It The app serves you ads disguised as emails.

It lags and stutters on powerful hardware. It interrupts you with pop-ups about new features you never asked for.

And if you decide you prefer the old Outlook, you'll be hounded with prompts to "try the new Outlook" until you give in.

Even if you resist entirely, you're still not free. Uninstall Outlook, and it will quietly reinstall itself with the next Windows update.

Disable it, and Microsoft will sync your settings from the cloud and turn it back on. Outlook's a manifestation of the Microsoft's worst habits:

constant nudging, endless telemetry, and an assumption that the company knows what's best for you.

The same attitude that bloats Windows has now infected your inbox.

Although I'm on Windows — and therefore tethered to Microsoft's ecosystem — I'll resist it wherever I can.

I don't need a daily reminder that I'm tolerating bad software out of necessity.

So if there's one area where I still have a choice, it's my email client, and it won't be Outlook.

Not when the alternatives are faster, cleaner, and simply better.

Don't let Microsoft convince you that Outlook is your only choice. It's not.

You deserve an email experience that's fast, clean, and free from manipulation. Microsoft's Outlook simply isn't that anymore.

How to Disable Siri on the iPhone and iPad

Disabling Siri can be achieved in a handful of steps. First, open the "Settings" app on your iPhone or iPad and then select the "Apple Intelligence & Siri" option.

On older devices that don't support Apple Intelligence, this will simply say "Siri."

Tap on the "Talk & Type to Siri" entry and choose "Off" and then toggle "Press Side Button for Siri" off too.

You can also disable "Type to Siri" if you see the option.

If you only want to disable Siri when your device is locked, you can toggle off "Allow Siri When Locked" on the previous screen instead.

When you disable both Siri's listening feature and Side Button access, you'll see a pop-up asking you if you really want to turn off Siri.

Read the warning (which states that HomePods will no longer recognize your voice and respond to personal requests), then tap on the "Stop Using Siri" button.

Siri has now been disabled on your iPhone and iPad.

It's also possible to **disable Siri on your Apple Watch** to achieve a similar goal. This is handy if you keep triggering the assistant by mistake,

since the default shortcut for doing so involves holding down the digital crown (which is easy to do by mistake).

To do this, launch the Watch app on the iPhone that's paired with your Apple Watch. Scroll down until you see Siri, then tap the "Listen for" option and choose "Off."

Now head back to the previous screen and disable "Raise to Speak" and "Press Digital Crown" to turn off Siri for good.

Disable Siri Requests and Suggestions

While Siri started out as a voice assistant for the iPhone and iPad, its role has significantly expanded over the years.

Siri is now used as a blanket term for Apple's smart suggestion features as a whole.

From app suggestions in search to smart notifications on the lock screen (which can be quite annoying), everything is handled by Siri behind the scenes.

You can turn these off if you don't want to see them, using the same "Siri & Apple Intelligence" (or just "Siri") section in the Settings app.

Once in the menu, swipe down until you see the "Suggestions" heading and then tap on the toggle buttons next to the following entries:

- Suggest Apps Before Searching
- Allow Notifications
- Show in App Library
- Show When Sharing
- Show Listening Suggestions

You can disable all or some of these, depending on your preference. You may also want to head into the "Announce Calls" and

- "Announce Notifications" sub-menus of the "Siri Requests" section to stop Siri from telling you who is calling or interrupting you with notifications when you're trying to listen to music.
- If ever you decide it's time to turn Siri back on, perhaps when Apple finally gets around to rolling out the big Apple Intelligence Siri update,
- head back to the relevant menu and turn these back on. You'll be asked to say a few things out loud so that Siri can recognize your voice.

One reason you might decide that Siri is worth enabling again is for smart home control. Apple's assistant may have a rocky reputation, but

Apple Home works surprisingly well with the powerful open-source smart home platform Home Assistant.

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.