



S C C C

Buderim Meeting Friday 24.10.2025 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

1. Q&A
2. Purchasing a New Laptop
3. Irfanview - how to create a slideshow.
4. 35mm slides - convert to JPG's

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

Sat. 25.10.2025

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.

Locked Out Of Your Gmail Account? Google's Recovery Contacts Feature Can Help

With a new Google two-factor authentication [code theft warning](#) hitting the headlines, the threat of being locked out of your

Gmail account has once again moved to the forefront of security-minded users of the world's most popular email platform.

Google itself has not only confirmed updates mitigating the latest 2FA threat, but has now gone one step further by introducing a new security feature.

This feature is designed to help if the worst happens and you find yourself locked out of your account due to hacker action, device loss, or password amnesia.

With attacks against Google accounts, and that means your Gmail account as well, spiking by 84% across the past year, [according to Google](#), with password-stealing email threats the prime culprit, taking [account recovery](#) seriously is long overdue if you have overlooked it so far.

Which is why Google is rolling out a brand new security feature called [Recovery Contacts](#) to reinforce the Gmail account

recovery precisely at those times of most stress when you need help immediately.

The Recovery Contacts setting enables Gmail users to choose trusted contacts, family members or close friends to provide help

if ever they find themselves locked out and unable to receive a recovery code for any reason.

Google Also Confirms New Gmail Android 'No Verification' Lock Screen Recovery Feature

The Gmail security updates are coming thick and fast, it would seem, and that's got to be a good thing.

The latest in the form of a confirmation from Eugene Liderman, Google's director of Android security and privacy, along with

John Gronberg, the product management director. "You can now regain access with your mobile number," the Google security and safety posting stated.

That might not sound much of an advance, but anyone who has been locked out of their Google account for whatever reason will surely be pleased to hear it.

After all, the loss of a smartphone, whether through an account or by theft, or even breakage, can be stressful enough without having to worry

about the impact that could have on access to your Google account and your Gmail as a consequence. "To make recovery on a new Android device easier,"

the posting confirmed, “we’re introducing Google's [Sign in with Mobile Number](#), which automatically identifies your accounts using your phone number.”

Like all good security features, this one does not add cumbersome hoops for you to jump through, but removes them instead.

All you need is the lock-screen passcode from your previous device for verification,” Liderman said.

Yep, that’s right; no password required. “We are introducing this gradually worldwide,” Liderman concluded, “watch for it on a phone near you.”

Similar to most people, I wasn't the biggest fan of AI when it started to pop up.

I thought it stifled creativity and made people more reliant on tools for even the simplest tasks.

And sure, I wasn't exactly wrong about that. Most people do indeed turn to ChatGPT for the simplest tasks.

But over time, I realized the more you resist AI, the quicker you're going to **get left behind**.

Since then, I've made it a point to try out every AI tool I come across.

I had accepted **ChatGPT's personality**. I'd tried countless custom prompts, memory tweaks, and advanced prompting techniques to make it better, and eventually gave up.

I thought changing anything would only make it worse, but today, I gave in and tried a feature I had ignored.

The result was dramatic. ChatGPT instantly stopped spamming me with pointless flattery at the start and redundant follow-up suggestions at the end of its response. It just answered what I asked and did what I told it to.

I asked the same question twice. See the difference for yourself. I'll reveal the simple fix now.

Go to **Settings → Personalization → Personality**, and switch ChatGPT to **Robot**.

That’s it. Save, and try your prompt again.

I'm not here to knock OneDrive (or maybe I am), but Microsoft OneDrive is not a good choice for backing up your Windows PC

unless you plan to pay for an upgraded storage plan. I was aware that Windows PCs set up OneDrive to back up files automatically.

However, I was unaware that this backup is, in fact, not a true backup. Ignorance is bliss.

What I mean by saying that Microsoft OneDrive isn't a real backup is this: OneDrive automatically saves all your files to OneDrive, **not your PC**.

So, instead of creating a legitimate cloud storage backup, you're actually just saving all your files to the cloud.

So the moment I got fed up with alerts that I was running out of OneDrive storage, I decided to go on a deletion spree.

Upon realizing that all the files I thought I was simply deleting from the cloud were, indeed, not saved anywhere on my PC.

After panicking, I went to the source, looking for help threads, and found various similar complaints that mirrored my experience.

I am not the only person who has [grown tired of OneDrive](#).

Unless you ensure in your PC's settings that it is not linking everything to OneDrive, this could happen to you.

Google has suddenly [confirmed](#) privacy initiatives “are being phased out.”

The Privacy Sandbox, now in its sixth year, has essentially ended just months after

Google confirmed tracking is here to stay and there are no viable alternatives.

Text attacks on Android and iPhone owners in America, Europe and elsewhere are totally out of control.

This [billion-dollar industry](#) now defrauds [millions of smartphone owners](#).

The malicious technologies that execute these attacks [originate in China](#) but impersonate your local DMV or delivery firm.

That's why they're ruthlessly effective.

"The threat of online scams and fraud is an ever-present reality in our connected world," Google warns its users, “and the volume of scams is only growing.

Nearly 60% of people globally have experienced a scam in the last year.”

Google says it will lock down all these texts "unless you explicitly mark the message as ‘not spam’.

And just like Apple, while filtering spam is important, the intent is also to capture dangerous scam texts in this same, widely deployed net.

Google has just [confirmed](#) “this protection is now available globally to all Google Messages users.”

Attackers have proven so adept at bypassing networks defenses, only a platform-level technology solution can address this now.

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.