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. Command Prompt? Power Shell? Terminal?
3. What's the Difference? Which Do I Want?

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.

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

A 'supercharged' scam threat is about to take Australia by storm, an AI expert has warned, with over one million people expected to be targeted.

Research by software development company **Airteam** has revealed that AI-enhanced phishing attacks could affect up to 1.18million people in
the next 12 months, marking a 372 per cent rise on the 250,000 Australians scammed in 2024.

Phishing is a type of online scam where criminals pretend to be trustworthy entities, often via email, text message, or fake websites,

to trick people into sharing sensitive information such as passwords, bank details, or credit card numbers.

A recent **Microsoft** report showed AI-automated phishing emails achieved a 54 per cent click-through rate compared to
just 12 per cent for standard attempts, making them nearly five times more effective.

The technology features sophisticated lures that even savvy internet users struggle to identify, and subsequently can prove up to 50 times more profitable.

'Everyone needs to be on their toes. **It's coming** and we need to be prepared.

'I really worry about older Australians, I worry for them because it happens so quickly and this stuff is really hard to identify.'

'Al has improved the quality of it (phishing attacks). Just making tiny changes to subject lines, preview texts,

or calls to action can really make significant changes in terms of how these emails perform,'

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.

Since the October 14th deadline for regular mainline **Windows 10 updates** has passed, though,
this will still confuse some users, and understandably so. In the context of a business, it's even worse,
as it could trigger unnecessary service desk calls and administrative work.
Thankfully, Microsoft has already chimed in to confirm that the issue was limited to the displayed message.
All affected devices, regardless of the warning, were continuing to receive their scheduled security updates.

Microsoft reported that it pushed a cloud-based configuration fix to resolve the issue for many affected

devices automatically, which should act as a stop-gap until a more permanent fix arrives in a future update.
You'll have to wait, though.

The new 2026 models of the **Motorola** G and Moto G Play offer a handful of incremental but appreciated
upgrades that **Motorola** hopes will make these affordable phones even more appealing.
You’re getting faster charging, a bigger battery, a better display, and some very cool color options this time around.
If you’re trying to save a buck, you don’t want to sacrifice too much,
and Motorola is once again stepping up to the plate with the dependable Moto G and Moto G Play series.
Both 2026 Moto G and G Play sport 6.7" 120Hz LCDs with 1,000-nit peak and Gorilla Glass 3.
Moto G has 50MP main/32MP selfie; G Play 32MP/8MP; both use quad pixel tech.
Both pack 5,200mAh; Moto G 30W charging, G Play 18W.
Both models are powered by the MediaTek Dimensity 6300 chipset and 4GB of RAM.
The Moto G has 256GB of storage, while the Moto G Play has 128GB.

We live our **entire lives connected to the web**, signed up for dozens of services using accounts.
Many of those accounts are so critical, that it's no exaggeration to say having them compromised could ruin your life,
or at the very least be an expensive and inconvenient disaster.

The good news is that, although there's no such thing as perfect security,
there are several things you can do that makes it much less likely your services will be compromised.

Use a unique password for every account
It's hard to remember a bunch of passwords, but a cardinal sin of cybersecurity is to use
the same password for multiple accounts. Why? Because this makes your password as safe as the
service provider with the worst data breach protection. Hackers know people like to do this,
so if they manage to breach a soft target, they'll check major accounts like Gmail or your
bank to see if you used the same password to log into those services.

Also, don't just use the same password slightly remixed,
since that is basically giving hackers the easiest dictionary attack on a silver platter.

Let a password manager handle the hard part

If you have lots of accounts, it makes sense to use a good password manager.
With the right software, you can generate, manage, and change your passwords with very little effort on your end. Many browsers have built-in password managers for free,
though some cybersecurity experts advise against using a browser password manager for fears of insecurities in the browser itself.

Turn on two-factor authentication (2FA) everywhere you can

A password alone, no matter how secure, just isn't enough to keep your accounts safe.
Two-factor authentication makes it so you need two different "keys" before gaining access,
and the two need to be unrelated. For example, a text message with a one-time PIN in addition to entering your password. It's orders of magnitude harder for a hacker to compromise both your phone and password than just one or the other.

So if 2FA is offered on an account, it's almost always better to make use of it.

You can add one or more **emergency contacts to your iPhone** so that they can be easily

contacted (or contact you) in urgent situations.

This takes five minutes to set up, but it could be one of the most important settings on your device.

An emergency contact is a contact that exists in your address book that has a few additional privileges compared to your other contacts.
There are two reasons to set up an emergency contact on your iPhone.
The first is so that they appear as a next of kin on your Medical ID.
This is accessible by strangers from your lock screen and contains information like your name, allergies,
blood type, and (once set up) people who should be contacted in the event of an emergency.
You can access your Medical ID by pressing and holding the power and volume down
buttons until the "Medical ID" slider appears.
You can also access it via the "Emergency" button on the passcode screen, or by holding the Side Button (not the digital crown) on an Apple Watch.

Your Medical ID is a vital iPhone safety feature that everyone you should be using.

If you don't see this option, you should head to the Health app and set it up first.

If you get into a situation where someone may want to contact an emergency contact,

they can easily do so from this screen without having to unlock your device.

The second reason to add emergency contacts is so that these contacts receive a message
whenever you use your device's "Emergency SOS" function.
This is accessed by pressing and holding the power button and volume button on an iPhone,
then sliding "Emergency SOS" or by pressing and holding the side button on an Apple Watch.
You can also elect to bypass your device's silent mode settings to allow a contact to sound an
audible alert on your device regardless of your settings.
You can do this for any contact on your iPhone, whether or not they are set as an emergency contact or not.

You can set an emergency contact via a contact card or using the Health app on your iPhone.
To do this using the contact card, launch the Phone app and tap on the Contacts tab, then select a contact.
You can also tap on the Recent tab and tap the small "i" button next to a contact's name.
Scroll down to the bottom of the contact card and tap the "Add to Emergency Contacts" button.

Regularly Back Up Data for Peace of Mind