S C C C

Buderim Meeting Friday 27.2.2026

Time - 12 pm to 3 pm

100 Buderim Pines Drive, Goodlife Centre Buderim

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. Audacity Sound File Editor/Recorder
3. Explaining USB Power Connecors

Replacement for BOM Radar - Rain Rate

Get e Prepared

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

Sat. 28.2.2026

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.

A certain deadline related to the **Windows Secure Boot** feature is approaching in mid-2026.
Before Windows loads, Secure Boot verifies the system's startup process.
But to do this, it relies on cryptographic certificates, and unfortunately, a lot of these long-standing Secure Boot certificates expire in June 2026.
This means systems that don't transition in time may be unable to accept future boot-level updates.
On PCs where future firmware or security updates rely on newer Secure Boot certificates, some devices may simply not start.
Microsoft has already started rolling out newer certificates, so there should be no need to panic.
However, you should understand how it all works to avoid any unpleasant surprises.

The trust system that decides whether your PC is allowed to boot

Before Windows, drivers, and antivirus software come into play, Secure Boot does its work.

Every time you turn on your computer, the system firmware uses a set of trusted certificates stored directly in UEFI firmware

to verify that critical boot components, primarily the Windows Boot Manager, have been signed by a trusted authority.

If the signature cannot be verified against a trusted certificate, the boot process is immediately terminated.

This verification is an important step in the chain of trust. Microsoft's private keys sign Windows boot components,
and the corresponding certificates are stored in the firmware's DB (authorized signatures database);

these certificates determine which bootloaders are trusted to run. The KEK (Key Exchange Key database)
guarantees that only a trusted entity can modify allowed bootloaders by holding certificates that control who can update the DB.
The significant point is that Secure Boot certificates have expiry dates.
After expiration, your PC's firmware can't rely on the expired certificates as a trust anchor.
This is an intentional security mechanism for limiting long-term exposure to compromised or outdated signing keys.
Since Windows 8, these three outgoing certificates have been the backbone of Secure Boot on Windows computers.
Microsoft UEFI CA **2011** is replaced by two certificates to improve security granularity.
While you may not expect every system that doesn't adopt the newer certificates to suddenly fail, they may be excluded from future Secure Boot updates or protections.

The ultimate Android remote app for TV

BT Remote is a free, open-source application developed by Atharok.
Because it is open-source, the source code is transparently available on GitHub for anyone to audit, and the app itself is conveniently hosted on both the Google Play Store and F-Droid.
It's a simple tool. It transforms your smartphone into a full-featured, full-screen remote control.
You get the numpad, arrow keys, home, back, volume bars, and dedicated media controls.
Best of all, it lacks those annoying, hard-coded Netflix and Disney+ buttons that are physically built into modern Google TV remotes — buttons you usually end up pressing by accident in the dark.
If you simply can’t be bothered to dig through the couch cushions for the physical remote, you can grab your phone and keep going.
That’s a great convenience, but it is far from the only perk this app offers.
The best bits of this remote app come from the two tiny buttons on the top-right corner.
Clicking the first brings up a touchpad on the bottom. Yes, you now have a Bluetooth mouse connected to your TV.
If you swipe on the virtual touchpad, you'll see a cursor — just like the Windows cursor — appear on your TV screen.
Now you can go straight to a menu without having to click through every other menu on the way.
The other button, with the keyboard icon, brings up a keyboard on your phone.
You can type whatever you want, and it'll type right into your TV.
I bet you type much faster with your phone than with a physical TV remote.
So, essentially, although the app is called BT Remote, it adds a full Bluetooth package of a mouse and keyboard to your TV as well.
The setup might be a bit confusing at first, my TV's Bluetooth didn't show up for my phone to pair automatically.
I can't tell if this is by design, but my TV's Bluetooth is almost always invisible.
Thankfully, the BT Remote app also allows you to pair using a MAC address.
The MAC address is the absolute Bluetooth address of your device.
On Google TV, you can navigate to the settings, then information, and find the Bluetooth MAC address to input it in the app.

Fake Chrome extensions look like popular AI assistants

The Chrome extensions identified as part of AiFrame look like legitimate
AI tools commonly used for summarizing, chat, writing, and Gmail assistance.
But once installed, they grant attackers wide-ranging remote access to the user's browser.
Some of the capabilities observed include voice recognition, pixel tracking, and email content readability.

Researchers note that extensions are broadly capable of harvesting data and monitoring user behavior.
AI-powered browser extensions continue to be a popular vector for threat actors looking to harvest user information.
Researchers at security firm LayerX have analyzed multiple campaigns in recent months involving malicious browser extensions, including the widespread GhostPoster scheme targeting Chrome, Firefox, and Edge.
In the latest one—dubbed AiFrame—threat actors have pushed approximately 30 Chrome add-ons that impersonate
well-known AI assistants, including Claude, ChatGPT, Gemini, Grok, and "AI Gmail." Collectively, these fakes have more than 300,000 installs.

Be careful what you install.

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