S C C C

Buderim 19.6.2026

Time - 12 pm to 3 pm

100 Buderim Pines Drive, Goodlife Centre Buderim

Nevil Eyre Android Phones & Tablets & Home automation

Tutorial Room Bill Maxwell

1. Q&A
2. Searching! Can't find where you saved that file? Use Everything to find it.
Looking for a name in a file? Use CONTENT: Search to find which documents have that name.
3. How to use my Table of Contents.

Replacement for BOM Radar - Rain Rate

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

Saturday 20.6.2026

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.

Caught in the SIM paradigm

In the end, the idea of eSIMs is a good one, but in practice it's not yet ready to fulfill the promise of a fully digital cellular access system.

At the very least, we need some sort of universal standard for what the sign-up and transfer process is for eSIMs.

Ideally, there should be no reliance on a third party to stand in your way, and a device-to-device eSIM feature should be standard.

In particular, moving eSIMs from iPhone to Android and vice versa needs to be a simpler process.

Carrier restrictions that have come over from physical SIMs to eSIMs need to be rethought.

Switching between eSIMs on the same device could do with some more refinement.

We are really hoping for is a system that isn't just a digital copy of how physical SIM cards operate.

We want a future where you can switch on a phone, scan for available carriers and just sign up with a username and password.

Just like Wi-Fi in a coffee shop. We've moved beyond needing SIM cards and phone numbers as factors for authentication.

With technologies like passkeys now a reality, there has to be a better way to handle mobile subscriptions.

The concept of needing to set a secure password has been hammered into our heads for so long, it barely warrants a mention.

And while some of us definitely go out of our way to make some passwords super secure, other passwords lie there forgotten for ages.

Wi-Fi passwords fall under that umbrella: they're often never changed, and if they are, they're made to be easy to remember.

Creating a strong Wi-Fi password is the bare minimum for protecting your network, but on its own, it simply isn't enough.

There's one more important login and password that you might be neglecting, even if you actually pay attention to your Wi-Fi password.

Most routers have two separate passwords, but most people are unaware of that fact. And yeah, it does get a bit confusing.

The first one is your Wi-Fi password, which is what you type in when you connect a phone, laptop, TV, or console to the network.

That's the password most people think about when talking about Wi-Fi.

The second one is the router admin password, and that's the one that actually lets you change how the router works.

It protects the settings page where you can rename the network, change the Wi-Fi password, update firmware, view connected devices, and tweak security features.

Changing your Wi-Fi password won't automatically change this admin login,

so it's entirely possible for your Wi-Fi password to be super strong while leaving the router's control panel protected by something unchanged since setup.

Default router admin passwords are often treated like a setup formality instead of a serious security measure.

Depending on your router and ISP, yours might be printed on a sticker or stored in an app.

Needless to say, a password that everyone can get access to at any given time isn't ideal. The same goes for leaving the password as "admin."

Default credentials only exist to make your router easy to set up, but they're not meant to keep your network safe for years.

If you never changed the admin password, anyone who can reach that login page has a much better starting point than they should.

A long, unique admin password stored in a password manager is a small change that takes no time at all, but it's an important security step.

Fake call detection

It's getting harder and harder to figure out what's real.

Scammers can use deepfake AI and spoofed caller ID to make you believe you're

answering a call from someone you know, like your mom, who you might give your credit card.

Google rolled out fake call detection in June as part of its Android Feature Drop,

and it's one of the more practical and useful security additions.

Caller ID was created to show you a number and a name,

not to prove the person holding the phone is actually the person that matches the information.

Scammers have exploited this loophole, called number spoofing,

by routing calls through software that can make any number appear in your Caller ID display.

The new development is called AI voice cloning.

Experts say AI audio deepfakes can be so realistic that most people can't tell the

difference between the AI and a real human voice.

Combine this with a spoofed number and you've got a prime way to get past any suspicions you might have.

If you see mom's number and hear your mom's voice, you likely won't think twice.

The scale is pretty significant, as well.

INTERPOL's March 2026 Global Financial Fraud Threat Assessment report cited impersonation

fraud as one of the leading contributors to over $400 billion in global losses.

The FTC logged $2.95 billion in impersonation scam losses in 2024 alone.

Instead of analyzing voices, Google's fake call detection works at the device level.

When a saved contact calls you and both of you are running **Google's native Phone app**,

the caller's device sends a confirmation signal in real time to verify the call is legitimate

and truly coming from the contact's device.

This digital handshake uses end-to-end encrypted RCS (Rich Communication Services) technology, keeping it completely private.

From Peter [Benefits of Books reading]

If you receive a threatening phone call, hang up immediately. Do not disclose personal details to the caller.
Never provide your personal or banking details to a person who calls you.
Never provide your financial PIN or account passwords to anyone.
Do not make any payments to the caller, either via phone, internet, or cash.
If you are suspicious about the credentials of a person on the phone, ask questions of them.
If they avoid answering or refuse to provide information, hang up.

Don't let scammers pressure you – scammers use detailed scripts to convince you that
they're the real deal and create a high-pressure situation to make a decision on the spot.
If you think you have provided your account details to a scammer, contact your bank or financial institution immediately.
Contact police immediately to report the incident.

Treat every email as suspicious.

To Recycle old PC's Old computers

Regularly Back Up Data for Peace of Mind