S C C C

Buderim 24.7.2026

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. PDF Tools - How to edit - and fill in forms.
3. What is the DARK WEB?
4. Why you should not click "Unsubscribe"?

Replacement for BOM Radar - Rain Rate

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

Saturday **25.7.2026**

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.

Your smartphone could be the weakest link in your online security portfolio.

We all know that phones hold some of our most personal and sensitive information, like messages, notes, photos, or videos.

However, they're also the gateway to much more crucial data — online banking systems, government accounts, or mobile ID cards.

This is the kind of information that, if compromised, could have life-altering effects, such as identity theft and fraud.

A simple device passcode or biometric isn't enough to protect your online banking apps.

To fortify your Android phone, you should keep your banking apps completely partitioned in a location bad actors can't even see.

Using Android 15 or newer, you can set up **Private space** to create a separate home screen environment that's isolated from the rest of your phone.

Take it one step further by hiding the private space entirely, and your banking apps will finally feel secure on your smartphone.

Setting weak passwords or shared devices aside for a moment, your banking app's icon living on an Android home screen is a security risk in itself.

There are many ways an online account can become compromised, but a common one is credential stuffing.

You use a username and password combination with one site, and a data breach or leak makes it public.

By now, a login credential you've used in the past has almost certainly been leaked, and websites like HaveIBeenPwned help you prove it.

Here's where things get tricky. If that username and password combination is for, say, a fast food chain's app,

you might not be too concerned about the credential leak. However, bad actors use credential stuffing to try these same login credentials on other,

more important sites. If you use the same password for multiple accounts, that's a huge problem.

If you use identical usernames or email addresses across multiple sites, that's not as big of an issue, but it still could be a cause for concern.

For anyone with malicious intentions, finding out which apps and services you use is half the battle.

If you place your banking app's icon on your home screen, you're broadcasting where a hacker needs to focus their attention to steal your identity or their cash.

On the flip side, if you don't put your banking app front and center on your smartphone, it could be harder to figure out which institution you use.

The more worrying situation is having your most important apps, like online banking software, secured by only a four- or six-digit device passcode.

If you use your phone's biometrics or password manager to store your online banking credentials, these are only as secure as the passcode that locks your device.

In other words, not secure enough to safeguard your life savings.
Private space doesn't just lock or hide your sensitive apps from the rest of your device — it's like a digital safe that exists separately from the rest of your Android phone.

Unless you've manually set it up in the Settings app on your Android device, you probably didn't know it's there.

To get started, open Settings → Settings & privacy → Private space. Then, enter your device's passcode to open the page.

While some routers are designed to lay flat, many modern residential solutions work best upright.

These routers typically have internal antennas that you can't see, and they are responsible for sending Wi-Fi signals throughout your home.

The direction of these antennas crucially determines the wireless signal path of your Wi-Fi.

Positioning the antennas correctly can avoid physical obstructions and improve wireless coverage,

while an incorrect placement can lead to interference, signal degradation, and dead zones.

The technical detail about antenna direction most people miss is that wireless signals radiate perpendicular to their actual positioning.

If you have router antennas pointing straight up, your wireless signals will be sent out horizontally.

Router antennas pointed to the side will radiate wireless signals vertically.

Usually, you want these signals to radiate horizontally — this sends Wi-Fi coverage outward and limits physical interference with obstructions,

like ceilings. However, if you have a single router tasked with providing coverage for an entire multi-story home, horizontally positioned antennas could be preferable.

Router and antenna placement is easy for advanced, prosumer networking gear. These enthusiast and enterprise-grade router models

often have external antennas that can be pointed in the direction of your choice, regardless of whether the router is physically standing up or lying flat.

The tricky part is positioning entry-level residential routers with internal antennas.

The only way to ensure the internal antennas are facing the right way is to change the orientation of the router itself.

Routers designed for vertical placement are made to radiate wireless signals horizontally.

These signals project evenly throughout your home, creating a line-of-sight connection with your devices.

Take a vertical router and put it on its side, and you're sending those wireless signals up and down instead.

The signals are going toward your ceiling and floor rather than throughout your home.

This creates speed and coverage problems that will leave you scratching your head.

This is because routers typically work best off the ground, at waist or eye level.

Think about it — the devices connecting to your router aren't living on the floor, so why should your router?

If the goal is to get your router sending wireless signals horizontally to your devices, placing it on the floor defeats the point.

Facebook is the one platform most associated with the aging millennial population and their boomer parents.

These days, most of the social media action happens on TikTok, YouTube and in messaging apps.

But there's one part of Facebook that deserves your attention and can legitimately make you money while cleaning out clutter from your house: **Marketplace.**

Porch pickup is common on Marketplace, but it runs entirely on trust, so a few precautions are worth it.

For anything higher-value, or with a buyer you can't vet, meeting in a public place is the safer move —

many police stations now have designated exchange zones for exactly this. And whenever you can, count the cash before the buyer leaves.

Most people don't pay much attention to Facebook nowadays. And I get it: as far as social networks go,

Facebook is the one platform most associated with the aging millennial population and their boomer parents.

These days, most of the social media action happens on TikTok, YouTube and in messaging apps.

Marketplace is best through the Facebook App.

Facebook has made a truly mobile-first shopping experience (unlike eBay, which is primarily designed to be used on a desktop computer overall).

The app makes it super easy to take photos of your item directly from your phone where you can also add a title, description, and fill in other details.

To sell something on Marketplace, just open the Facebook app > tap the Marketplace tab on the bottom > tap Sell > Create listing.

There are some limitations

You first must have a Facebook account in good standing and be over 18.

If your account is new, you are likely to face restrictions in your ability to use Marketplace.

When it comes to selling stuff around your house, Facebook Marketplace is genuinely fantastic and in most ways superior to eBay.

How do you know someone is a serious buyer? They're likely to send you a substantive question, or provide you with a specific pick-up window.

Sometimes, you'll have someone request a quick phone call so that they can determine if you're a serious seller.

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

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.