

S C C C

Including Bill's WEB PAGE

Buderim Friday 6.11.2026

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. Office Programs.

BOM Radar - Rain Rate

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

Saturday. 7.11.2026

8.30 to 11.30 am
M C C Meridan Plains
70 Springs Dr. QLD 4551

here

Hands on Help - Windows, Linux and Chromebooks

Please wear your Name Tag.

For many, the internet is feeling less secure these days, thanks to generative artificial intelligence (AI) tools making it easier than ever to exploit hidden security flaws.

PHP incident is a great example. PHP is one of the main technologies that run in the background, supporting more than 70% of the websites we use every day. A critical vulnerability prompted many organisations to take their websites offline to secure them.

The national cyber security agency, Australian Signals Directorate, is also warning of rapidly evolving cyber threats. It issued more than 4,400 notifications about potentially malicious cyber activity in 2025–26, almost 80% more than the previous year.

In the wrong hands, AI tools can threaten the underlying systems the internet relies on, outpacing many organisations' capability to patch them.

First, let's establish **there's no big switch that turns the internet off.** Why? Because the internet is not just one big box of technology. It's not like your smartphone or TV that you can power on and off.

Instead, the internet is a global network of computers and other devices connected to each other, and it supports a collection of services.

Think of the applications you use every day, from browsing social media to sending emails or banking. For these services to run, computers use network infrastructure to exchange data.

For example, when you look at a website hosted on a server in the United States, data travels between your computer or smartphone and that server through network connections.

These connections may use physical cables that run between continents to connect networks together, as well as wireless links (such as wifi) and satellites.

This network is like the roads between Melbourne and Brisbane. One road may be blocked, but there will usually be alternative routes, although there may be some travel interruptions or delays.

Losing access to one internet system doesn't necessarily mean losing access to others. But what happens when many of these systems depend on the same underlying technology?

These are known as shared dependencies. Think, for instance, of how we use Google or Microsoft accounts to access school, university or workplace services.

A failure in the shared sign-in system could prevent us from accessing email, Word documents and online learning platforms at the same time.

A complete internet blackout is highly unlikely, given its underlying infrastructure.

Interruptions to specific services, on the other hand, are both plausible and likely to continue to increase.

If there was a cyber attack on healthcare systems, for example, a clinic might continue consultations but Medicare claims might be delayed.

A transport or banking app might be unavailable due to security risks, while trains could still run and card payments continue to work, assuming these services were not affected, as well.

Patching or recovery from cyber incidents can range from routine repairs to systems or equipment, to investigating compromised systems, which may involve complex digital forensic work.

The reach of an outage depends on which shared systems fail and whether alternatives are available.

The examples below show how widely some digital services and technologies are used, and how a failure could affect our lives.

Microsoft says threat actors are ahead in the early AI race

Microsoft says cyberattackers are currently benefiting from artificial intelligence faster than defenders, allowing threat actors to speed up vulnerability discovery,

malware development, and post-compromise activity while security teams struggle to keep pace.

Google's Gemini could soon access any file on your macOS device, open apps, browse the web, and perform actions without asking for permission every time.

The China-linked ransomware group Warlock targeted a water utility, a telecom provider, a regional government body, and a university by exploiting SharePoint vulnerabilities to gain initial access.

The setup is incredibly simple.
All you need to do is download Blip on both devices and enter your email address.
That's about it.

Once both devices are set up, you can start **sharing files** between
them seamlessly.
Another small but incredibly useful detail is **Blip lets you send entire folders with their structure intact.**
The file transfer happens whether both devices are on the same network or not.
The most convenient thing about it is that you don't even have
to wake the other device or accept the file transfer.
If both devices are using the same email address,
the transfer happens automatically. And if you're sharing files with someone else,
Blip makes that easy too. You can simply search for their device by entering
their name or email in the search box.
It almost feels like you're using an instant messaging service.

A useful built-in feature on most Android phones is the ability to **convert any photo into a PDF.**
Most gallery apps have a PDF conversion feature that works similarly across different devices and Android versions.
Just open any photo, press the three-dot menu, and tap the Print icon.
Now just select the Save as PDF option, tap the PDF button, and choose where you want to save the file.
To save a web page as a PDF in Google Chrome, open the web page, tap the three-dot button, then tap Share, and finally tap Print.
Now, all you have to do is save the web page as a PDF.
To save an email as a PDF in Gmail, open the email you want to save, press the three-dot menu, tap the Print button, and save the email as a PDF.

Please keep the mobile apps, desktop software, operating systems and browsers updated.

Regularly restart your smartphone

If it's unexpected or urgent, slow down… no quick-pay links, open your bank or service app directly instead.

1. 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.

2. Assume anyone can be fooled Treat every email as suspicious.

Use strong logins like passkeys, and keep less personal info public (private Facebook profiles)

From Peter Benefits of Books reading About Scams

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.