

S C C C

Including Bill's WEB PAGE

Buderim **Friday** **13.11.2026**

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. AI for Dummies
3. Typing Special characters that are not on your keyboard. £ ® 😂

BOM Radar - Rain Rate

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

Saturday. **14.11.2026**

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

here

Please wear your Name Tag.

Computer security often devolves into magical thinking.

That's unfortunate because the reality is that most of the things you can do to protect yourself online are about simple psychology and basic human behavior.

When a business network is compromised with ransomware, the culprit is rarely an evil genius hacker. The source of the problem is usually far more mundane:

Someone was fooled by a clever bit of social engineering.

For anyone who's responsible for training others to avoid being online victims, the secret is not to explain how buffer overflows and code injection work.

Instead, help those people focus on how to approach PCs with a healthy dose of skepticism and build up some basic situational awareness.

The natural human reaction when you see a potential threat is to panic and immediately try to do something to solve it.

If you get an email alerting you that your credit card's about to be charged $480 to renew your non-existent Geek Squad subscription or that your computer is

infected with ransomware, you might be tempted to call the toll-free number in that email.

That will, of course, connect you to a call center staffed by bad actors who will happily take your credit card details and process some real charges.

Scammers thrive by making people panic. Take the time you need to figure out what the real threat is before you do anything.

Don't open unknown attachments

Many potential security threats arrive in the form of email attachments. Sometimes they're executable files, but these days they're just as likely to be Word documents,

PDFs, or HTML files. They might be capable of running exploit code, or they might be simply an attempt to convince you to enter credentials for an email or bank account.

If you receive an attachment from someone you don't know, the last thing you should do is open it. Even if the attachment appears to be from someone you know,

it pays to be cautious, especially if the message is unexpected. The sender's account information might be spoofed, or their account might be compromised.

Don't click unsolicited links, either.

Social engineering works by exploiting people's trust. A scammer who puts even minimal effort into a phishing attempt can do a creditable job of mimicking a legitimate

email and crafting links that look close enough to the real thing to fool you.

If you receive an email that makes you think, "Hmmm, that doesn't look right," your spidey sense is working. Trust it.

And even if the message doesn't have any obvious red flags, it's still OK to be suspicious, especially if you're being asked to click a link to do something you didn't ask for.

When in doubt, don't click that link; instead, use a bookmark you've saved for the site in question or type the URL directly to do whatever you need to do.

You don't need to pay for security software.

The security software industry wants you to be afraid. As part of that effort, they try their best to convince you that the core protections built into your PC, Mac,

or mobile device cannot possibly be as good as the product they sell.

Don't mess with a perfectly good PC (or Mac)

When it comes to keeping your computer secure, I have a slightly different take on the classic management advice: "If it ain't broke, don't break it."

Drive-by exploits might get all the headlines, but the sad fact is that most malware arrives on PCs because someone willingly, even eagerly, chose to install it.

Maybe they downloaded a cracked program from a sketchy download site, or maybe they followed a sponsored link from a search engine and grabbed a program

that included a bundle of adware or even malware in addition to the app they were looking for.

The obvious solution? **Don't install random apps.**

Use a password manager.

In fact, using a password manager makes it easier to navigate the modern internet and keeps you safer. If you've been putting off this task because you think it's too difficult,
which you can implement in 30 minutes or less.
Oh, and while you're at it, **turn on two-factor authentication, too.**

Microsoft PC Manager is a free system optimization and utility app developed by Microsoft for Windows 10 and Windows 11.
It acts as a lightweight, first-party alternative to third-party maintenance tools like CCleaner.
For most everyday Windows users, Microsoft PC Manager is a better, safer, and cleaner alternative to the free version of CCleaner.
It is 100% free with no locked features or upgrade nags.
• Health Check: Scans your system in one click to identify temporary files, cache, and quick fixes.
• PC Boost & Smart Boost: Clears temporary files, system cache, and frees up RAM; Smart Boost can automatically optimize memory usage when it runs high.
• Storage Management: Handles deep cleanups (including app caches for tools like Steam and Epic Games), large file searches, and **duplicate file management.**
• Process & Startup Management: Lets you view and end resource-heavy background processes and control which apps launch when Windows starts up.
• Protection & Pop-up Management: Integrates with Windows Security for threat scans, checks Windows Updates, and helps reduce app pop-up interruptions.
• Toolbox: Provides quick access to built-in Windows utilities like a screenshot tool, calculator, and notepad.

Meta has quietly introduced a way for Australians to stop the tech giant from training its AI on their user data, but the company never announced it,
leaving the choice effectively hidden for more than a year.
There was a furious public backlash in mid-2024 when it was revealed Meta was using photos, posts and comments stretching back to 2007 to train its AI.
At the time, Australians were told that, unlike EU citizens, they could not opt out because of weaker privacy protections.
To opt out of Meta's AI training go to your Instagram profile page,
tap the tree horizontal lines in the top right hand corner of screen to access the Settings menu.
Scroll down to the bottom and tap on Privacy center.
Submit the form and you will get an email confirming the company will not use their public data to train its AI in the future.
It also explains that accounts set to "private" are already exempt, as are all private messages, and accounts listed as belonging to users under 18.

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.