
# S C C C

**Buderim Meeting Friday 5.12.2025**

**Time - 12 pm to 3 pm**

**100 Buderim Pines Drive**, Goodlife Centre Buderim
Admission - $4

**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. All files on your computer have an Associated Program that will Open or Display that file.
If there is no Associated Program, you will not be able to open or run that file.

A good example of this is when someone sends you an Email Attachment that you can't open.
This is because you don't have the program on your computer that created the Attachment.
All files on your computer and identified by their file type (Extension).
This File Extension tells the computer which program to open and there are settings where you can
change the file extension and sometimes you pick wrong and things go bad.

Replacement for BOM Radar - Rain Rate

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

**Sat. 6.12.2025**

**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.**

**Christmas / New year break information 2025 / 2026**
Last meeting Buderim 12 December 2025
First meeting Buderim 16 January 2026 at Goodlife Centre

Last meeting Meridan Community Centre 13 December 2025
First meeting 17 January 2026 at Meridan Community Centre

Microsoft has spent the last four years trying to get everyone to upgrade to Windows 11, but not everyone has made the switch.
With Windows 10 reaching "End of Life" last month, many are considering ditching Windows altogether.
If you've felt the urge to finally check out a Linux alternative, you're not alone—and the numbers prove it.
**Zorin OS** has always been one of the most compelling Linux distros for anyone jumping ship from Windows.
That's because it was designed specifically to make switching to Linux from Windows as smooth as possible.
This approach seems to be working as the team announced over one million downloads of its latest version, Zorin OS 18.
And of those downloads, over 78% are coming from Windows. Not all of those people are going to stick with Zorin OS forever,
but it still shows a huge number of people are feeling unrest about the future of Windows.
So what makes it such an appealing option for Windows users? Zorin OS is built on Ubuntu, but it mimics Windows in many ways.
There are multiple Windows-like layouts to choose from, the file explorer resembles Windows Explorer, there's right-click content menus,
familiar Control Panel organization, integrated OneDrive support, and more. Of course, it's different in many ways too.

Zorin OS 18 features heavy web-app integration, allowing you to use the new Progressive Web App installer to turn services
like Office 365 or Google Docs into standalone applications.
Compatibility with Windows apps has also been upgraded in this release.

While it still uses compatibility layers like Wine, the user-facing experience has been tweaked so more
applications should run right out of the box without you needing to spend time fiddling with settings.

It should also be mentioned that Zorin OS can be a great Linux distro for Mac users as well. Zorin OS Pro includes layouts
that can transform the interface into a macOS lookalike. These layouts give you a lot of control over how everything looks and feels.

With Microsoft continuing to double down on AI features and generally being a bit user-hostile with Windows 11, it's easy to see why so many people are looking elsewhere

According to security researchers at Google's Project Zero, several popular anti-malware tools have had several high-severity vulnerabilities.
These range from insecure network filters to flawed file parsers. Because your antivirus runs with full system privileges, any vulnerability
within it is a golden ticket for an attacker. For example, in 2024, Tech Monitor reported on malware that exploited a vulnerability in an Avast/AVG kernel driver, allowing attackers to disable the security software and target other parts of the system.
The point isn't that all antiviruses are insecure. However, when you add such a massive and highly privileged code base to your system,
your computer isn't automatically "safer." So, when I uninstalled my antivirus, I removed a complex system component that could have been exploited.
The constant pop-ups from some antivirus tools are akin to marketing tools. I received upgrade prompts and a recurring "Your PC may be

at risk!" banner, which created security fatigue. After a while, you get used to these warnings and pop-ups.
You assume it’s all upselling and stop paying attention, putting your computer at risk when there’s an actual threat

**Social engineering attacks** are probably still among the most used ways to actually infect a computer or steal someone's data.
A well executed social engineering attack can have some pretty nasty consequences. This one even involves a fake Windows Update screen to round things up.
Cybersecurity researchers have uncovered a sophisticated evolution in "ClickFix" social engineering attacks, where threat actors
are now combining realistic fake Windows Update animations with advanced social engineering techniques to compromise systems.
In case you don't know what a ClickFix attack is, its goal is to trick the user into performing an action that security software typically blocks when performed automatically.
In these new variants, victims encounter full-screen browser pages mimicking a critical Windows security update or a "human verification" captcha.
The page instructs the user to press a specific sequence of keys to resolve an error or verify their identity. Unbeknownst to the user, JavaScript running on the malicious site has already copied a malicious command to their clipboard. When the user follows the key-press instructions (often involving pasting into the Windows Run box or Command Prompt), they inadvertently execute the attacker's code.
It's actually pretty smart, and that's why it's scary. What makes this specific campaign distinct is the use of steganography to conceal
the malware payload. Rather than downloading a recognizable malicious file, the attackers hide the code inside the pixel data of PNG images.
Huntress researchers explained that the malicious code is encoded directly within specific color channels of the image.

To a casual observer or a basic security scan, the file appears to be a harmless image. However, the attack chain includes a .NET assembly known as a "Stego Loader." This loader is responsible for parsing the image, extracting the encrypted payload from the pixels, and decrypting it in memory.

The way this works is that you visit a website displaying a fake full-screen error, such as a stuck Windows Update or a "verify you are human" check.

Background scripts on the site secretly copy malicious code to your computer's clipboard.

The screen instructs you to open the Windows "Run" prompt and paste the text to "fix" the issue, and once you hit "enter," the command downloads a seemingly harmless image file, which actually contains the malware that's then decrypted by the Stego Loader.

The entry point function initiates calls to 10,000 empty functions to exhaust or confuse analysis tools before executing the real payload.

You or I probably wouldn't be victims of this. But think of an older person who might be fooled by this—maybe by clicking on the wrong link online.

A disaster waiting to happen. To prevent this, you can disable the Run box on your grandpa's PC, but there's not a lot else you can do.

### 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

**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.