



[S C C C](#)

Buderim Meeting Friday 3.10.2025 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

1. Q&A
2. A review of my web page selecting a few topics at random to talk about.

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

Sat. 4.10.2025

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.

Find Facebook Help From Dedicated Pages

One more way you can contact Facebook directly is through forms. Facebook makes several forms available that you can use to submit requests or report problems with your account or someone else's.

Here are some of the forms that you can use on the site:

- Photo Removal Request: To remove your own, your child's, or another adult's photo from the platform, use this form.
 - Account Was Disabled: If your account is disabled, use this page to request Facebook to review the account.
 - Change Name: Use this form to change your first, middle, and last name in your account.
 - Confirm Identity: You can confirm your identity on Facebook by submitting a valid ID card using this form.
 - Medically Incapacitated or Deceased Person: To make changes to an account whose account holder can't do it because of medical reasons, use this form.
 - Report Violation: To report trademark or copyright violations, fill in this form.
 - Report Underage Child: If a child below the age of 13 is using Facebook, use this form to report that child's profile to Facebook.
 - Child Data Request: Get the data Facebook has on your child with this form.
 - Report a Page Unavailable Error: If you encounter a "Page Unavailable" error on Facebook, use this form to let Facebook know about it.
- After completing a form, Facebook will review your request and take appropriate action or get back to you asking for more details.

Find Online Guides for More Help

We understand the pain of not being able to get an important query answered by Facebook.

You can check out [our Facebook archive](#) to access all the articles we've published about Facebook.

Most Windows 11 Users Don't Need an Antivirus: Here's Why

While conventional wisdom says you need an antivirus to stay safe online, most Windows 11 users may not need a third-party antivirus at all.

As long as you keep your system updated and practice safe browsing habits, Windows 11's built-in protections are enough to keep you secure online.

Microsoft Windows Security has come a long way. Once the butt of jokes, it's now a robust security solution built into the operating system.

Since Windows 10, it has matured into a comprehensive suite, combining Microsoft Defender Antivirus, Windows Firewall, and

Smart App Control to block potentially dangerous files and threats. Here's what the security suite consists of:

- Virus & threat protection: Traditional and behavioral malware detection with manual scan options.
- Firewall & network protection: Controls network traffic and blocks unauthorized connections.
- App & browser control: Includes SmartScreen filter to block malicious sites and downloads.
- Device security: Manages hardware security features like secure boot and core isolation.
- Account protection: Manages sign-in options and monitors account safety.
- Device performance & health: Shows a quick overview of your device's health and potential issues.

But how effective is it really? In the [January and February 2025 AV-TEST evaluations](#),

Microsoft Defender Antivirus earned a perfect 6.0 score across all categories—protection, performance, and usability.

This translates to excellent protection against advanced malware attacks, including web and email threats, minimal system impact ranging from 1% for downloads and copying files to 23% for website launching, and zero false positives.

Windows Security works quietly in the background, automatically updating its virus and threat definitions without interruption.

In my experience, it's impressively resource-efficient. Even during active background scans, I've only observed CPU usage between 11% and 14%, with no noticeable impact on my system's performance.

Edge users can benefit from the integrated SmartScreen filter that actively scans websites and downloads to detect

anything sketchy before it reaches their computer. Even if you are using Chrome, Firefox, or Opera, Microsoft's got you covered with Network Protection.

However, you'll see system alerts instead of browser warnings. Plus, all these modern browsers have built their own

pretty solid security features anyway, so you're protected regardless of which one you're using.

While it may sound familiar, [don't mistake Windows Security for Microsoft Defender](#), which is now a standalone app and part of the Microsoft 365 suite.

This separate offering provides additional features like VPN and identity monitoring, acting as a centralized dashboard to view and monitor all devices connected to your account.

Best Security Practices Can Beat Any Antivirus

Even the best antivirus can't protect you if you don't follow basic security practices. By applying common sense, you can significantly improve your online security.

For instance, don't download unknown or suspicious attachments, and avoid downloading pirated software or movies from unknown sources that are often riddled with pop-ups and automatic redirects. Keeping your system up to date with the latest Windows updates is the single most important security measure you can take to secure your system.

Many successful attacks exploit vulnerabilities that were patched months or even years ago. The same logic applies to your browser and applications.

Those update notifications may be annoying, but they often include critical security patches.

Another security weakness for many is passwords. Instead of recycling the same password for all your critical accounts, use unique, complex passwords.

Consider using one of the best password managers to handle the complexity of generating and remembering strong passwords for multiple accounts.

Third-Party Antivirus Software Has Its Issues

Third-party security tools aren't without merit, and depending on the provider, they can offer some useful features.

Some, like Avast, provide webcam monitoring to alert you of suspicious access attempts. Most premium security suites now include identity theft protection and password leak monitoring, scanning the dark corners of the internet for your compromised data.

Extended parental controls and built-in VPN protection are valuable features that add additional layers of security beyond what's available in Windows Security.

More importantly, a third-party antivirus can give you a second opinion on your system's overall health.

However, it's worth noting that Windows automatically disables its built-in security features when it detects a third-party security app installed.

That said, these additional features can easily bloat your computer and impact system performance.

Free third-party antivirus often act as a marketing funnel for their premium offerings, with consistent upgrade reminders

and privacy concerns with user data collection, resulting in an overall poor user experience.

I haven't used any third-party antivirus in the last few years, at least not on my personal computer. I do have one on my test

machine because it's part of the job. My decision stems from disciplined security practices and how well the built-in Windows Security solution has improved over the years.

Ultimately, the choice is yours. If you need the extra bells and whistles that third-party antiviruses offer, the premium might well be worth it.

However, for most of us who practice good security hygiene, keep their systems updated, and avoid unsafe digital practices, the built-in Windows Security provides more than enough protection for everyday use.

Regularly Back Up Data for Peace of Mind

Aussies are being warned about a [new email scam](#) doing the rounds, which claims to be sent by an online security software company.

If you feel you have fallen for a scam, contact IDCARE, a free government-funded service which will work with you to develop a specific response plan to your situation, and support you through the process.

<https://www.idcare.org/>

1. Phishing Emails: In a phishing scam, the attacker will send their target a message claiming to be an official, trusted party.

This kind of urgent communication works well in pressuring the recipient to comply with the senders request.

2. Remote Desktop Protocol. Simple: **Don't allow Remote Connections.**

3. Flash Drives. **Don't allow strange Flash Drives to be used on your PC..**

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.