



S C C C

Buderim 22.5.2026

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. File Management
3. Internet Archive.

Replacement for BOM Radar - [Rain Rate](#)

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

Saturday

23.5.2026

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.

WinGet is a **Windows package manager** that allows you to search, install, remove, and update Windows applications through a single command line application.

For most Windows users, a command line seems like a blast from the past.

Most people never open PowerShell or Command Prompt. But you shouldn't overlook WinGet.

Having a tool that gives you this much automation, ease of installation,

and friction-free updates is worth stepping out of your comfort zone for.

Looking for a particular type of application?

You can just search the directory and install it directly from there.

It's like the Windows Store, without the "store" part.

Package managers exist in other operating systems, so this isn't anything new,

but if you're a Windows user, it could change how you manage your applications.

- WinGet is a Windows package manager that simplifies app installation and updating via the command line.
- With WinGet, you can easily search, install, and update Windows apps, making management seamless and efficient.
- By providing direct files without installers, WinGet offers safe app updates with no risk of unwanted bundled software.

It can bulk-update all your currently installed apps to the latest version through a single command.

One of the biggest problems with installation packages is that you're never sure

if you're getting what you want from them.

They may include unwanted bundled software or even malware embedded inside the installer.

Even if you scan with Windows Defender, there's a chance malware will slip through the cracks.

WinGet avoids that by giving you the files directly without packaging them in an installer.

It's the safest way to update your applications.

winget list: This gives you a list of all your currently installed applications,

where the executable is on your device, current and available update versions, and where it comes from.

- **winget upgrade** : WinGet is one of the most powerful app update tools out there. From the list function, you can see which apps need updating, and process that directly by entering the app name in the parameter field. Alternatively, you can upgrade all your apps by using
- **winget upgrade -all** .
- **winget show** : This command gives you an overview of a particular application. This includes a readout of the current version, WinGet's description, and many other details like the type of installer the program uses.

WinGet is one of the coolest features that Windows 11 ships with that many people overlook.

YouTube without Google.

NewPipe is a safe alternative to the YouTube app that lets you access

It has absolutely no ads, no For You page, and no Shorts feed.

You can search the YouTube library without an algorithm pushing irrelevant videos in the results.

You can subscribe to channels, create playlists, and browse comments.

This app also lets you play videos in the background, download them in high quality, add videos to queues, and make playlists.

What you can't do is leave comments because it doesn't connect to a Google account.

If you want to build a fresh YouTube feed from scratch

or if you waste too much time on YouTube,

I recommend this app.

Resetting your laptop in the event you've been locked out. You'll need to activate an Advanced Startup, which is done by holding down the Shift key while clicking the Restart button on the Windows login screen. Keep Shift held down until the screen reads 'Please wait', then release.

Select 'Troubleshoot', then 'Reset this PC', and follow the same instructions.

Scammers love to impersonate businesses you trust in hopes of convincing you to fall for their cons. One tactic they use is to call you pretending to be from your bank or financial institution.

The goal is to trick you into sending them money or revealing your account details. Now, Google is rolling out a new security tool that aims to combat these types of spoofed calls.

Designed to protect you from financial theft or account compromise, the feature aims to detect spoofed calls. Here's how it works.

First, you need to **install your bank's app** on your Android device. When you receive a call that seems to be from your bank,

Android queries the app for confirmation to determine if the call is legit. If the app finds that no one from the bank is actually calling you, the call is disconnected.

Spoofing a number from a trusted business like your bank isn't that difficult. Scammers use internet-based calling systems to spoof their caller ID so it appears they're calling from a different number. This type of caller ID spoofing can easily turn you into a victim of financial fraud.

To kick off this new feature, Google said that it's working with select banks and financial institutions to implement these verified forms of financial calls.

Rolling out to devices with Android version 11 or higher in the coming weeks, the verification will start slowly.

Scammers will try to intercept the one-time passwords (OTPs) from your text messages to snoop on your personal accounts.

To thwart this, Android will now automatically hide these security codes for three hours from most apps, making sure that the OTPs are safe from unauthorized access.

Launched in 2024, analyzes the behavior of apps via on-device AI and then alerts you if an app seems suspicious. With the latest enhancements,

this feature will warn you about any suspicious behavior that could also be dangerous or harmful.

The protection will also extend to such activities as SMS forwarding in which an app forwards a message to another phone number.

Another existing security feature, Advanced Protection warns you about apps that try to change or hide their icons, a potential sign that they could be malicious.

With Android 17, Advanced Protection will also remove access to the accessibility service for all apps not labeled as accessibility tools.

Google's Find Hub already helps you track down a lost or stolen phone, allowing you to lock it remotely.

Currently, your device can be unlocked by anyone who knows its passcode or PIN. With Android 17, you'll be able to require that the phone be

unlocked only through biometric authentication, such as your facial or fingerprint scan.

The goal is to prevent thieves who discover your passcode from unlocking your phone.

Many apps ask for your location so they're able to work effectively. These include navigation apps that need to know your exact whereabouts.

Coming in Android 17 is a new location button that lets you share your precise location but only for specific tasks while an app is open.

As an example, you could use this to track down a nearby restaurant without granting permanent access to your location each time you open the app.

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) so scammers have less to mimic.

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.