



S C C C

Buderim 29.5.2026

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. Back Up Program - GFI -
Will show how to download, Install and setup.
3. File Explorer
4. Using Snipping Tool to record a Video.

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

Discussion on iPad and iPhone functions.

Limited help with basic Apple Mac computers.

Saturday

30.5.2026

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.

OCR (optical character recognition) in the Snipping Tool

If you need to quickly extract some text from an image, the Windows Snipping Tool can help you with that.

It's known as the **Text Actions feature**. Open the Snipping Tool and **take a screenshot** of the image that you want to extract text from.

If the photo is already on your PC, you can right-click it and open it in Snipping Tool.

After that, press the Text Actions button from the top menu.

You can then click the "Copy All Text" button to copy all the text in the picture.

You can also manually select text using your mouse and copy only specific portions.

If there is any sensitive information in the picture such as phone numbers or emails, you can redact it too.

You've likely heard of VPNs and antivirus software as essential tools that help maintain your online security and privacy, but **firewalls** often get little to no attention.

However, they're just as important when it comes to protecting your devices and data, especially given the growing number of cybersecurity risks.

If you value your online safety, there are five reasons a personal firewall is a must-have.

A firewall works by acting like a filter between outside traffic sources and your device.

Without a firewall, your network and device are open to every attempted connection, including malicious ones.

Even if you practice safe browsing habits, a skilled hacker could gain unauthorized access to your system without you even knowing.

With a firewall, though, incoming and outgoing data is continuously scanned and filtered based on pre-determined security rules, ensuring that only trusted IP addresses can access your device.

This gives you an extra layer of protection against malicious users and more control over your network and devices.

A firewall can protect you against cyber threats, including malware and viruses. However, you shouldn't consider it a substitute for [antivirus software](#).

There are [differences between how a firewall and antivirus work](#); when used together, they can complement each other and offer comprehensive security.

However, a firewall is still a good first line of defense against known malware and viruses.

Blocking unauthorized traffic, including suspicious IP addresses with harmful data packets and malicious software, can stop bad traffic from reaching your device.

Modern operating systems come with built-in firewalls, but this [type of firewall](#) offers limited protection, typically only extending to the device the OS is installed on.

This is seldom sufficient, given that home networks today are connected to all kinds of IoT devices. For instance, a couple of smart TVs, a camera,

and a few phones connected to my home network at all times. These devices lack robust security features like a built-in firewall, making them an easy target for cybercriminals.

The good news is that keeping your device free of spammy pop-ups is fairly easy with a firewall, which blocks unwanted traffic.

Although firewalls can help maintain online security, keep in mind that they cannot protect your device against all types of cyber attacks.

Defragmentation Can Be Bad News For Your SSD

Defragmentation is not recommended for SSDs because it can potentially decrease the performance and lifespan of the drive.

This is because SSDs have a limited number of write cycles, and defragmentation can use up a significant portion of these cycles,

resulting in reduced performance over time.

In addition, defragmentation can be time-consuming, especially on larger SSDs. Due to how SSDs read and write data,

asking the drive to essentially

erase and rewrite itself can saturate its resources as it shuffles data to and from its internal cache as it writes to its memory cells.

So what are your options if defragmentation is off the table and your SSD is still feeling sluggish?

While SSDs typically optimize themselves, these are the methods that keep SSDs operating at peak speeds:

Trimming: Trimming is a process that helps maintain an SSD's performance by deleting unused data blocks and

making them available for reuse.

This can help prevent the SSD from becoming cluttered with unused data, slowing it down.

Your operating system likely already performs the

TRIM command or some more modern equivalent without your knowledge.

Modern SSDs are smart enough to perform this type of maintenance **independently without even being told.**

Overprovisioning: Overprovisioning is setting aside a portion of the SSD's capacity for use by the drive's firmware.

This can help improve the drive's performance and lifespan by reducing the number of write cycles and providing

additional space for the drive to store data.

In most cases, the drive has automatic built-in overprovisioning, but some drive makers let users modify the amount

of overprovisioning using a proprietary utility app.

Keeping the drive clean: Keeping the SSD free of unnecessary files and programs can also help to improve its performance.

This can be done by regularly deleting unused files and uninstalling unnecessary programs.

This is one of the reasons larger SSDs are often faster than smaller SSDs.

If you receive a threatening phone call, hang up immediately. Do not disclose personal details to the caller.

Never provide your personal or banking details to a person who calls you.

Never provide your financial PIN or account passwords to anyone.

Do not make any payments to the caller, either via phone, internet, or cash.

If you are suspicious about the credentials of a person on the phone, ask questions of them.

If they avoid answering or refuse to provide information, hang up.

Don't let scammers pressure you – scammers use detailed scripts to convince you that they're the real deal and create a high-pressure situation to make a decision on the spot.

If you think you have provided your account details to a scammer, contact your bank or financial institution immediately.

Contact police immediately to report the incident.

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.