S C C C

Buderim 3.7.2026

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 Systems Explained
3. Windows 10 Extended Security Updates

Replacement for BOM Radar - Rain Rate

Discussion on iPad and iPhone functions.

Limited help with basic Apple Mac computers.

Saturday 4.7.2026

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.

Charging to 80% Preserves a Battery's Lifespan

Most rechargeable devices use a lithium-ion battery. This battery chemistry does not like to be fully discharged,
meaning it's not good to let your battery hit 0% for reasons beyond the device cutting off on you. Do it often enough, and you harm the battery.
Less obviously, charging to 100% isn't ideal either. While charging to 100% doesn't inherently cause any problems,
leaving the battery at a high state of charge **puts unnecessary stress on the battery and shortens its lifespan.**
Batteries like to be in a Goldilocks zone of between 20-80%, not too low and not too high. Unfortunately,
it's unrealistic to expect us to babysit our devices in order to preserve their batteries. That's what software is for.
Fortunately, some Windows laptops come with the ability to set a charging threshold.

Sometimes this option is available in desktop software, and other times you need to dive into the BIOS.

MacBooks have a feature called Optimized Battery Charging that also sets charging thresholds.

Not all USB-C cables are the same

USB-C looks simple because the plug is the same shape, but the cable behind it can be very different. Think of USB-C as just the “port type,” not a guarantee of speed or capability. Some cables are built only for basic charging, while others can handle fast charging, high-speed data, or even video for a monitor—and a lot of cheaper or older cables only support a subset of those.

For charging, the key difference is how much power the cable can carry. Basic cables might only handle slow charging, while better ones support USB Power Delivery (often written as USB-PD), which lets devices like iPhones, iPads, MacBooks, and Android phones charge much faster.

If your phone is charging slowly, it’s often because the cable (or the charger) can’t deliver enough power, even if it physically fits.

For data transfer, cables vary just as much. Some are limited to older USB 2.0 speeds (fine for charging, but slow for moving photos or backups), while others support much faster standards like USB 3 or beyond. Two cables can look identical, but one might take minutes to transfer files while the other takes seconds.

To connect to a display, the cable needs to support “video over USB-C” (often called DisplayPort Alt Mode or Thunderbolt).

Many basic charging cables simply don’t include the wiring needed for video, so your laptop or tablet won’t detect the monitor at all, even though the cable works fine for charging.

To stay out of trouble, it helps to look for a few clues when buying or using a cable ...

If you need fast charging, look for USB-PD support and higher wattage ratings (like 60W or 100W). (Power Delivery)

For fast data, check for USB 3.x or higher.

For monitors or docking stations, look for cables labeled for video, DisplayPort, or Thunderbolt.

If a cable came bundled with a device, it’s usually designed for that device’s main use, but may not do everything else.

When in doubt, slightly more expensive, well-labelled cables from reputable brands tend to save a lot of frustration compared to generic ones that don’t clearly state what they support.

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.

Be Connected

From Peter Benefits of Books reading

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.

Treat every email as suspicious.

To Recycle old PC's Old computers

Regularly Back Up Data for Peace of Mind