



[S C C C](#)

Buderim Meeting Friday 22.8.2025 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. The Cloud
3. Google Applications
4. **How Strong is your Password?**

Discussion on iPad and iPhone functions.

Limited help with basic Apple Mac computers.

Caloundra Meeting - Sat. 23.8.2025

8.30 to 11.30 am

70 Springs Dr, Meridan Plains QLD 4551

[here](#)

Please wear your Name Tag.

Send Password-Protected Documents With Office Suites

When you prepare a contract, budget, or business pitch, Microsoft Office and LibreOffice make password protection a built-in step.

You keep control over who accesses your sensitive information by following simple steps in programs you already know.

To lock down a Microsoft Office document, open your file and click on **File > Info > Protect Document > Encrypt with Password**.

Enter your password and confirm it. Office then encrypts your whole document with AES security. No one opens it without the password, period.

LibreOffice, a popular free suite among students and pros, offers a nearly identical method.

When you go to save your work, check the **Save with Password** option. LibreOffice then prompts you to type a strong password,

which it applies across the entire document using advanced encryption. Although it costs nothing, LibreOffice's built-in security matches or surpasses many paid solutions.

Remember, if you forget your password, neither Microsoft nor LibreOffice can recover the document for you.

Save passwords somewhere reliable, such as a free password manager app. Both Office suites have improved their encryption over the years, so run the latest versions for the best security. By using Office or LibreOffice, you avoid the risks of sketchy third-party tools while getting strong, trusted protection.

Free two-factor authentication apps usually come with a catch. They have limited features, poor sync, or questionable security.

But Proton Authenticator breaks this rule, and it's better than most paid alternatives I've used.

Proton Authenticator Solves Google's Biggest Security Flaw

I've used various two-factor authentication (2FA) apps over the years, but many—including Google's—have a glaring flaw.

The lack of secure, encrypted backups has always been a point of failure. Your 2FA codes get stored on Google's servers without end-to-end encryption.

Proton Authenticator solves this issue by encrypting everything before it leaves your device. It offers automatic, end-to-end encrypted backups and secure syncing across all your devices, including desktop.

Security Features That Actually Matter

Proton Authenticator covers the basic security features well, though some features work better than others in practice.

App lock with biometric authentication prevents access to your codes if someone grabs your phone, and the fingerprint prompt works reliably.

It is open source, unlike any other mainstream authenticator. That means security researchers can audit how data is handled,

which is usually one of the reasons why people prefer open-source software and apps. That's genuinely useful since you're not just trusting marketing claims about encryption.

If you want to add a code manually, the algorithm supports SHA1, SHA256, and SHA512 cryptographic hashes,

plus both time-based one-time password (TOTP) and STEAM authentication types. Additionally, it offers the option to adjust the code length

between six and eight digits and choose the time interval of 30 or 60 seconds. This flexibility helps when services use non-standard settings.

Offline functionality works as advertised. Your codes generate locally without needing internet connectivity.

Most authenticator apps handle offline generation fine, but it's still a crucial feature.

Besides, the automatic backup system creates encrypted snapshots by keeping only the last five backups.

The restore process worked smoothly when I tested it.

The Import Process Is Painless

Switching authenticator apps doesn't have to be tedious.

Proton Authenticator handles imports better than expected. To import codes from other authenticators, go to Settings and select the authenticator that you have been using.

The import screen supports major authenticators, including Google Authenticator, Bitwarden Authenticator, LastPass Authenticator, and several others.

The process involves exporting from your current app and importing the file into Proton Authenticator. If you are switching from Google Authenticator, the export button creates a QR code that Proton Authenticator scans directly. However, you'll see import warnings appear next to Authy and

Microsoft Authenticator, indicating compatibility issues since they don't allow direct TOTP exports.

You should verify that imported accounts work before deleting anything from your old authenticator, just to be safe.

The imported accounts retain their original names and issuers, so you won't lose track of which code belongs to which service.

However, there's a limitation that you can't selectively import specific accounts. It's all-or-nothing for each authenticator app, which

might be inconvenient if you only want to migrate certain codes.

Cross-Platform Sync Finally Works the Way It Should

Most authenticator apps sync across platforms. Google Authenticator finally added cloud sync but without end-to-end encryption.

Microsoft Authenticator syncs well, but ties you into their ecosystem.

Proton Authenticator handles sync across all major platforms—Android, iOS, Windows, macOS, and Linux.

That's more comprehensive platform coverage than Google or Microsoft Authenticator.

The sync setup requires a Proton account, which makes sense given the encryption requirements. Once enabled, your codes appear almost instantly on other devices.

The encryption means your synced data remains private even from Proton's servers.

That's the key difference from Google Authenticator's approach, where your codes exist in plain text on Google's infrastructure.

Desktop availability matters more than you might expect. When your phone battery dies or you're working on a computer,

having codes accessible without grabbing another device is genuinely convenient. Most authenticator apps skip the desktop entirely.

The sync toggle in settings shows which account handles your encrypted data, making it clear where your codes get stored.

You Don't Need a Proton Account (But You Should Get One)

Proton Authenticator works even without creating a Proton account. You can generate codes, use offline functionality, and access all basic features without signing up for anything.

However, you'll miss out on the main advantages, which are encrypted sync and automatic backups, both of which require a Proton account.

Without one, you're essentially using a local-only authenticator app, which defeats much of the purpose.

The real question is whether you want deeper integration with Proton's ecosystem. If you want to use a security-focused email service like Proton Mail

, ProtonVPN, or Proton Drive, adding the authenticator makes sense since everything works together better. For most people, the free Proton account provides enough functionality to make the authenticator worthwhile without committing to their broader ecosystem.

Two-factor authentication apps have been disappointing, often with poor sync, closed source, or both.

Proton Authenticator finally gets the fundamentals right, and it's also free to use without any ads. That is why it's recommended.

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.