

Ditch the Password, Own the Passphrase

Overview

Passwords are dying — not because they stopped working, but because computers got terrifyingly good at guessing them. This page explains why PBR is moving to **passphrases**, what the Australian Cyber Security Centre (ACSC) actually recommends, and how to build one in under a minute.

Stop using `Winter2026!`. Start using four random words strung together, like `correct horse battery staple`. Longer beats clever, every time.

The Maths Is Not on Your Side

Modern cracking rigs can attempt billions of password guesses per second. Short "complex" passwords — the classic capital-letter-number-symbol combo — fall fast because they're short, even with the symbols thrown in. Length, not complexity, is what actually slows an attacker down.

Credential	Length	Approx. time to crack*
<code>Winter26!</code>	9 characters	Minutes to hours
<code>Tr0ub4dor&3</code>	11 characters	A few days
<code>correct horse battery staple</code>	28 characters	Centuries+

**Illustrative only — actual crack times depend on hashing method and attacker resources, but the pattern holds: length wins.*

Password vs Passphrase — What's the Difference?

	Password	Passphrase
Structure	Short string, mixed characters	Several random words, spaces allowed
Example	P@ssw0rd1	purple duck potato boat
Easy to remember?	Not really	Yes
Easy to crack?	Yes	No, if genuinely random

What the ACSC Actually Says

This isn't a PBR opinion — it's straight from Australia's national cyber security authority (ACSC, part of the Australian Signals Directorate) and the Information Security Manual (ISM):

- **Go long:** aim for a passphrase of **4 or more random, unrelated words** totalling **at least 14-15 characters**.
- **Random beats meaningful:** the words should have no logical connection to each other and no connection to you (no pet names, birthdays, football teams).
- **Skip the sentences:** a grammatically correct sentence, a movie quote, or a song lyric is easier to guess than it feels — attackers use these exact sources as cracking dictionaries.
- **Don't force frequent changes:** the ACSC now recommends **against** mandatory periodic password resets (e.g. every 30 or 90 days) purely for the sake of it, because it pushes people toward small, predictable tweaks (Summer2025! → Summer2026!). Change your credential when you suspect it's been compromised, not on a fixed calendar.
- **Use MFA wherever it's offered** — a great passphrase is still stronger with a second factor behind it.

Further reading: [cyber.gov.au – Set secure passphrases](https://www.cyber.gov.au/set-secure-passphrases)

Building a Good One in 60 Seconds

1. Pick **four (or more) words** that have nothing to do with each other. Think of the most random things you can — an animal, an object, a colour, a place.

2. **Don't** pull them from a well-known quote, lyric, or saying.
3. String them together with spaces, hyphens, or just jam them together: tractor lemon violin harbour.
4. Optional: swap a letter for a number or add a symbol somewhere if the system requires it — but don't rely on this for strength, the word count is doing the heavy lifting.
5. Never reuse it anywhere else, and store it in **1Password** rather than memory or a sticky note.

□ Good Examples

- giraffe pixel thunder mango
- orbit-cactus-ferry-42
- quiet volcano bicycle jelly

□ Weak Examples (Avoid These)

- Password123! — short, predictable pattern
- IloveMyDogRex2026 — personal info, guessable structure
- tobeornottobe — a real, well-known quote
- correct horse battery staple — great as a teaching example, but now so famous it's in every cracking dictionary on earth. Use the idea, not this exact phrase!

Quick Reference Card

Rule	Guidance
Minimum length	14-15+ characters
Word count	4 or more random words
Reuse	Never — unique per account
Storage	1Password only — not memory, not sticky notes, not a text file
When to change it	On suspected compromise — not just because a calendar says so
MFA	Always enable where available

Related Pages

- [Keeping Your Account Secure](#)
 - [How To Use 1Password](#)
-

Sources

- Australian Cyber Security Centre – [Set secure passphrases](#)
 - Australian Cyber Security Centre – [Why it's time to ditch your one password for passphrases](#)
 - Australian Government Information Security Manual (ISM) – Guidelines for System Hardening, passphrase control
-

Revision #3

Created 2026-07-28 05:31:28 UTC by PBR_Documentation

Updated 2026-07-28 05:33:29 UTC by Dylan Healey