Unique password creation

Even with biometric login options and password-less technologies becoming more common, passwords still sit behind many core business systems.

Cyber criminals often rely on:

- Reused passwords from past data breaches
- Guessable passwords based on names or roles
- Poor password hygiene across multiple systems

Your password must:

- At least 12 - 16 characters
- Include numbers and symbols
- Use a mixture of upper and lower case letters
- No common phrases or associations
- Not reused anywhere else

Using the same password across multiple platforms is one of the biggest security risks for organisations. If one service is compromised, attackers will often:

- Try the same password on email accounts
- Target finance or admin systems
- Attempt access to Microsoft 365, Google Workspace, or cloud services

Password aims:

S!lent-Penguin-84^River

Password123!

Long passwords made up of random words are often more secure - and easier for users to remember - than short, complex strings. For businesses, every system should require a unique password, especially: Email accounts, admin, privileged user accounts, remote access tools, finance, HR platforms