Keeping Your Account Secure

Overview

Your PBR account gives access to email, files, financial systems, and customer data. Keeping it secure is your responsibility — and one of the most important things you can do to protect PBR.

Strong Passwords

- Use a **long passphrase** — three or four random words are more secure than a short complex password (e.g. *correct-horse-battery-staple*)
- Never use your PBR password on any other website or service
- Never share your password with anyone — including IT staff. IT will never ask for your password

---

Multi-Factor Authentication (MFA)

MFA adds a second layer of security to your account. Always approve MFA prompts yourself — if you receive a prompt you did not initiate, **deny it immediately** and contact IT Helpdesk, as someone may be attempting to access your account.

See: Multi-Factor Authentication (MFA)

Lock Your Screen

Always lock your screen when stepping away from your computer — even briefly.

- **Windows shortcut:** `Windows key + L`
- Your screen will also lock automatically after a period of inactivity

---

If You Think Your Account Has Been Compromised

Contact IT Helpdesk **immediately** if you:

- Receive MFA prompts you did not initiate
- See emails in your Sent folder you did not send
- Cannot log in with your normal password
- Accidentally entered your password on a suspicious website
- Accidentally clicked a link in a suspicious email

The faster we know, the less damage can be done. There is no shame in reporting — acting quickly is what matters.

IT Helpdesk: helpdesk@pbr.org.au

Approved Devices Only

Only access PBR systems on PBR-issued or IT-approved devices. Do not log into PBR systems on personal computers at internet cafes, libraries, or shared kiosk devices.

Revision #2
Created 2026-05-08 05:36:37 UTC by PBR_AI
Updated 2026-05-08 05:45:34 UTC by PBR_AI