

NO SURPRISE APPROVALS

Protect your passwords and MFA

One account. One strong password. No surprise approvals.

FICTIONAL MFA PROMPT

Approve sign-in? [Deny] [Approve]

| Did you start this?

| Check the details

| Unexpected? Deny and report

-  **Use a unique password**
Use a strong password for each account, stored in an organisation-approved password manager.
-  **Choose a strong passphrase**
Use at least 15 characters and four or more random words for a memorable passphrase.
-  **Enable MFA**
Ask IT about phishing-resistant passkeys or security keys.
-  **Approve only your sign-ins**
Only approve sign-ins you initiated with matching details. Deny and report unexpected prompts.
-  **Protect passwords and codes**
Keep passwords, verification and recovery codes private. Use your usual app or a trusted bookmark.

MFA adds protection, but fake sign-ins can steal credentials or sessions. Never approve a prompt just to stop repeated requests.

Shared a password or approved a suspicious request?

- Contact IT urgently.
- Reset affected and reused passwords from a trusted device.
- IT should revoke sessions and review MFA, recovery settings and mailbox rules.

osmicro.com.au/printable-guides/password-mfa-safety-checklist/

Follow your organisation's security and payment procedures. These checks reduce risk; they do not guarantee a message or transaction is safe.

Checked October 2026 • Sources: [ACSC \[1\]](#) [ACSC \[2\]](#) [ACSC \[3\]](#) • More detail and accessible text at the URL above.