revolution
your IT partner

// Making your business perform better.

Are We Basically Secure?

A plain-English cyber baseline for New Zealand businesses

If you can confidently tick most of these, you're in good shape.
If not, you'll know exactly where to focus.

1. Updates aren't optional [ ]

- Computers, servers, firewalls, and applications are supported and regularly updated.
- Old or unsupported devices are identified and removed.
- Updates happen automatically.

2. Logins are protected (even if passwords leak) [ ]

- Multi-Factor Authentication (MFA) is enabled on email, cloud apps, and remote access.
- Admin accounts have extra protection.
- The business does not rely on passwords alone.

3. Backups are tested — not just turned on [ ]

- Backups run automatically.
- Data restores have been tested and confirmed.
- Backups are protected from deletion or ransomware.
- Recovery time expectations are understood.

4. Access is limited to what people actually need [ ]

- Staff are not local administrators unless there is a genuine business reason.
- Admin access is limited, reviewed, and documented.
- Accounts for ex-staff are removed promptly.

5. Problems wouldn't go unnoticed [ ]

- Security events are logged centrally.
- Alerts exist for unusual or risky behaviour.
- Issues would be detected quickly, not months later.

6. There is a simple 'what if' plan [ ]

- There is a clear first point of contact if something looks wrong.
- Critical systems are identified and prioritised.
- The plan fits on one page.

7. Staff know what to be cautious about [ ]

- Staff are aware of suspicious emails and requests.
- There is basic security awareness training.
- Suspicious activity is reported, not ignored.

This checklist reflects widely accepted cybersecurity best practices for New Zealand businesses and aligns with guidance from CERT NZ and the National Cyber Security Centre.