Microsoft 365 Tenant Hardening Checklist

1. Create Multiple Global Admins

- At least two Global Admin accounts.
- Use different devices and MFA methods.
- Avoid personal Microsoft accounts.

2. Create a Break-Glass Admin Account

- Global Admin role.
- MFA disabled intentionally.
- Long random password stored securely.
- Excluded from Conditional Access.
- Alert if sign-in occurs.

3. Register Multiple MFA Methods

- Authenticator app.
- SMS.
- Backup phone.
- FIDO2 security keys.

4. Issue Security Keys (FIDO2)

- One primary key.
- One backup key stored securely.

5. Enable Self-Service Password Reset (SSPR)

- Enable in Entra.
- Require two authentication methods.
- Verify registration.

6. Document Everything Securely

- Admin accounts.
- MFA methods.
- Break-glass credentials.
- Security key locations.
- Conditional Access exclusions.

7. Avoid Using First Admin for Daily Work

- Convert initial admin to backup or break-glass.
- Use standard accounts for daily work.

8. Set Up Alerts for Admin Activity

- Role changes.
- Break-glass sign-ins.
- MFA changes.
- Password resets.
- Conditional Access changes.

9. Test Recovery Annually

- Break-glass login.
- Secondary admin login.
- SSPR flow.
- Security key login.
- Conditional Access exclusions.