Cyber Security Essentials

for Business Owners · by Chewing IT

Practical protection you can put in place this month

More than 80% of breaches start with a predictable failure — a reused password, an unpatched laptop, a phishing click. You don't need an enterprise security budget to shut the door on most of them. The ten habits below cover the biggest risks for Central Coast, Newcastle and Sydney SMBs, and most take a morning to implement.

01 Turn on MFA everywhere

Multi-factor authentication on email and admin accounts blocks ~99% of account-takeover attacks. Use an authenticator app (Microsoft Authenticator, Authy) — not SMS — wherever you can.

02 Use a business password manager

Every account gets a unique, long password stored in a vault like 1Password. Eliminates reuse, makes offboarding staff instant, and turns password hygiene into a non-issue.

03 Patch everything, automatically

Turn on auto-updates for Windows/macOS, browsers, Office and line-of-business apps. Unpatched software is how attackers get in after a phishing click. No exceptions for 'the one PC that can't reboot'.

04 Back up, then test the restore

3-2-1 rule: 3 copies, 2 media, 1 off-site and immutable. Microsoft 365 is NOT backed up by default — you need a third-party tool. A backup you've never restored is just hope in a folder.

05 Train staff on phishing monthly

Short, regular training + simulated phishing emails turns your biggest risk into your best sensor. Clicks are coaching moments, never punishments.

06 Harden your email

Set up SPF, DKIM and DMARC records so attackers can't impersonate your domain. Block auto-forward rules and legacy authentication in Microsoft 365 — both are attacker favourites.

07 Separate admin accounts

Nobody should browse the web, check email, or open attachments while logged in as a domain or Microsoft 365 admin. Create separate, MFA-protected admin accounts used only when needed.

08 Know what's on your network

Keep a current inventory of every device, user and SaaS service. You can't protect what you don't know exists — and ex-staff accounts are a ransomware gift-wrap.

09 Run real endpoint protection (EDR)

Replace traditional antivirus with an EDR — Bitdefender, Sophos or Defender for Business. Pair it with 24/7 MDR if you can; humans-in-the-loop stop attacks your tooling misses.

10 Write a one-page incident plan

When something goes wrong at 2am, who do you call? Document your MSP, cyber insurer, and backup admin contacts. Print it. Tape it to the fridge. Practise it once a year.

Want the checklist done for you?

Chewing IT runs a FREE Microsoft 365 Security Assessment — 95+ checks across identity, mail, files, devices and audit. Written report, yours to keep, no obligation.

Book at chewingit.com.au/contact

Chewing IT

ABN 42 628 833 330

Central Coast 02 4339 4789 · Sydney 02 8419 0940 · Get in touch via chewingit.com.au/contact

chewingit.com.au