



SME Digital Advisor

Plain-English advice on digital risk

FAQ · 12 CARDS

FAQ Flashcards

The 12 questions every owner asks, with plain-English answers.

Reference site for SME owners. Free. No sign-up.

Companion to andrewreaassociates.com

smedigitaladvisor.co.uk

FAQ #1 OF 12

Do we really need a CISO?

Almost certainly not, for a typical SME. A “virtual CISO” (fractional — a few hours a month) is plenty for most businesses under ~100 staff.

smedigitaladvisor.co.uk

FAQ #2 OF 12

Is Cyber Essentials enough?

It's a sensible *floor* — not a ceiling. Achievable, defensible, and increasingly required. But it doesn't address backup testing, incident response, AI use, supplier security, or training.

smedigitaladvisor.co.uk

FAQ #3 OF 12

How often should we change passwords?

Less often than people think, if you have MFA. NCSC moved away from forced rotation. Current advice: long passwords, unique per account, password manager, MFA on top.

smedigitaladvisor.co.uk

FAQ #4 OF 12

Should we ban USB sticks?

Most SMEs should at least restrict them. Disable unknown USB mass-storage; allow through an approval process.

smedigitaladvisor.co.uk

FAQ #5 OF 12

BYOD or company devices?

Company devices are easier to secure. If you do BYOD, you must have MDM and a clear policy. Many SMEs end up with company laptops, BYOD phones with MDM.

smedigitaladvisor.co.uk

FAQ #6 OF 12

Is our antivirus enough?

Probably not on its own. Modern threats bypass signature-based antivirus. The current category is EDR. Microsoft Defender for Business (bundled with M365 Business Premium) is good enough for most SMEs.

smedigitaladvisor.co.uk

FAQ #7 OF 12

Can we just back up to OneDrive / SharePoint?

No. They *sync* files; they don't back them up. If ransomware encrypts the originals, the encrypted versions sync to the cloud. Use a dedicated 3-2-1 backup tool that covers M365.

smedigitaladvisor.co.uk

FAQ #8 OF 12

Should we let staff use personal Gmail or Dropbox for work?

No. Creates data-protection, security, and continuity problems.

smedigitaladvisor.co.uk

FAQ #9 OF 12

Is cyber insurance worth it for a £2m turnover business?

For most businesses at that scale, yes — with caveats. The biggest value is usually the incident-response retainer bundled in.

smedigitaladvisor.co.uk

FAQ #10 OF 12

When does a 5-person business need a 'real' IT person?

Almost never as an employee. What you need is: someone in the business who owns IT decisions and a reliable MSP for execution.

smedigitaladvisor.co.uk

FAQ #11 OF 12

What's the difference between Microsoft 365 Business Standard, Premium, and Enterprise?

Business Standard is the core productivity suite. *Business Premium* adds the security tooling almost every SME should have. *Enterprise* tiers are for >300 users or specific compliance needs.

smedigitaladvisor.co.uk

FAQ #12 OF 12

Is two-factor by text message OK?

Better than nothing, much worse than an authenticator app. SMS is vulnerable to SIM-swap attacks.

smedigitaladvisor.co.uk