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. What you need is: someone responsible (could be you), competent help (could be your MSP), and an outside eye annually.

FAQ #2 OF 12

Is Cyber Essentials enough?

It's a sensible *floor* — not a ceiling. Cyber Essentials covers five controls. It's achievable, defensible, and increasingly required. But it doesn't address backup testing, incident response, AI use, supplier security, or training. Treat CE as “table stakes” that you build on.

FAQ #3 OF 12

How often should we change passwords?

Less often than people think, if you have MFA. NCSC guidance moved away from forced regular password changes years ago — they make people pick weaker passwords. Current advice: long passwords (three random words), unique per account, password manager, MFA on top.

FAQ #4 OF 12

Should we ban USB sticks?

Most SMEs should at least restrict them. Disable unknown USB mass-storage on managed laptops, allow through an approval process. “Don't plug in USB sticks you found” is more useful than “no USB allowed.”

FAQ #5 OF 12

BYOD or company devices?

Company devices are easier to secure and to defend in a Cyber Essentials assessment. If you do BYOD, you must have Mobile Device Management on phones and a clear policy. Many SMEs end up with company laptops, BYOD phones with MDM.

FAQ #6 OF 12

Is our antivirus enough?

Probably not on its own. Legacy antivirus catches known viruses by signature; modern threats are missed. The current category is EDR. Microsoft Defender for Business (bundled with M365 Business Premium) is good enough for most SMEs.

FAQ #7 OF 12

Can we just back up to OneDrive / SharePoint?

No. OneDrive and SharePoint *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 explicitly covers M365 (Veeam, Acronis, AvePoint, Datto).

FAQ #8 OF 12

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

No. Both create data-protection problems (personal data leaving your tenant), security problems (no admin oversight, no MFA enforcement, no audit log), and continuity problems.

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 that's bundled in. Read what's covered (and excluded), understand the insurer's requirements (MFA, backups, training), and then decide.

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. Below ~50 staff, “owner of the relationship” + “capable supplier” is the right pattern.

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 — Defender for Business (EDR), Intune (MDM), conditional access. The price difference is small for what you get. *Enterprise* tiers are for >300 users or specific compliance needs.

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. Use an authenticator app (Microsoft Authenticator, Google Authenticator, Authy, 1Password) for everyone; consider physical security keys for admins and directors.