UnderPin IT

FREE GUIDE

The Plain English Guide to Cyber Security for UK SMEs

Written for UK business owners, not IT departments. No acronyms without explanation. No technical jargon. Just a clear picture of what the real risks are, what they cost, and what to do about them in the right order.

43%
of UK businesses experienced a cyber breach or attack in 2025
UK Cyber Security Breaches Survey 2025, DSIT/Home Office

93%
of cyber attacks started with a phishing email
UK Cyber Security Breaches Survey 2025, DSIT/Home Office

78%
of SMEs have no formal incident response plan
UK Cyber Security Breaches Survey 2025/2026, DSIT/Home Office

Why every UK business is already a target

Cyber security is not about building a fortress. It is about making your business a harder target than the business next door. Most cyber criminals are not sophisticated state actors. They are opportunists running automated tools that scan millions of businesses looking for easy entry points. The good news is that the most effective protections are not expensive or complicated. They are just rarely done.

The five threats that matter most

Phishing	An email, text, or call designed to trick someone into handing over a password or clicking a malicious link. Responsible for 93% of successful cyber attacks on UK businesses. No technical skill is required to fall for one.
Credential Stuffing	Criminals buy lists of leaked usernames and passwords from previous data breaches and try them on other services. If your staff reuse passwords, this is a real risk. Checking your exposure takes 72 hours.
Ransomware	Malicious software that locks you out of your own systems until you pay. The average cost of a cyber incident in the UK is now over £7,500, with the average remediation taking more than four days.
Business Email Compromise	A criminal gains access to or impersonates a business email account and uses it to redirect payments or steal data. Often goes undetected for weeks.
Insider Risk	Former employees with active system access. Contractors who retained credentials. Staff who unknowingly share data in ways that breach GDPR. Most businesses have more open doors than they realise.

Five controls that block the majority of attacks

Cyber Essentials is the UK government's recommended security baseline. It covers five controls that, if implemented correctly, prevent the majority of common cyber attacks. Only 5% of UK businesses hold the certification. The controls themselves are not complex. The barrier is usually awareness, not cost.

1	**Firewalls** A firewall controls what traffic can enter and leave your network. Most businesses have one but many have never reviewed whether it is configured correctly.
2	**Secure Configuration** Devices and software should be set up securely from the start. Default settings on routers, laptops, and cloud services are almost always insecure.
3	**User Access Control** Staff should only have access to the systems and data they need to do their job. Admin rights should be restricted to people who genuinely need them.
4	**Malware Protection** Anti-malware software on all devices. 81% of UK businesses now have updated malware protection. But installation alone is not sufficient without regular updates.
5	**Patch Management** Keeping all software and operating systems up to date. Under Cyber Essentials v3.3 (April 2026), high-risk vulnerabilities must be patched within 14 days. Most businesses have no formal patch process.

The single most impactful thing you can do today

Turn on multi-factor authentication (MFA) on every business email account and cloud service. MFA means that even if a password is stolen, a criminal cannot access the account without a second verification step, usually a code on your phone. Under Cyber Essentials v3.3, MFA on every cloud service is now a mandatory requirement. Currently, 53% of UK businesses do not have comprehensive MFA in place.

Source: UK Cyber Security Breaches Survey 2025/2026, DSIT/Home Office

What GDPR means in plain English

UK GDPR is not just a compliance exercise. It requires that any business handling personal data takes appropriate steps to protect it. The word 'appropriate' is deliberate. It means the ICO will judge your response against what a reasonable business of your size and risk profile should have done.

You must know what data you hold	Where is customer data stored? Who has access to it? How long do you keep it? If you cannot answer these questions, you are already at risk.
You must report breaches within 72 hours	If personal data is lost, stolen, or accessed without authorisation, you are legally required to report it to the ICO within 72 hours of becoming aware. Most businesses do not have a process for this.
Healthcare carries the highest risk	The health sector reported more self-reported data breaches to the ICO than any other sector between 2023 and 2025. Patient data is classified as special category data under GDPR, carrying enhanced obligations.
Board-level accountability	Only 31% of UK businesses have board-level responsibility for cyber security formally assigned. Article 32 of UK GDPR expects senior management to be able to demonstrate how they protect data, not just that they have tools in place.

What to do this week, this month, and this quarter

THIS WEEK
☐ Turn on MFA on all business email accounts and cloud services.
☐ Check whether former employees still have active system access.
☐ Run a free dark web check on your primary business email domain.

THIS MONTH
☐ List every software subscription and IT contract your business pays for.
☐ Review who has admin rights across your systems.
☐ Identify who is responsible for IT decisions at board level.

THIS QUARTER
☐ Book a Technology Baseline Audit to map your full estate.
☐ Consider Cyber Essentials certification if you work with NHS or public sector clients.
☐ Establish a formal process for removing access when staff leave.

Want a clear picture of where your business stands?

The UnderPin IT Cyber Health Score

A half-day remote review that produces a clear, jargon-free traffic-light report across five areas: identity and access, email security, endpoint protection, patching, and backup. Fixed fee. £495.

Book at underpin-it.co.uk

Or email greig@underpin-it.co.uk

Fixed fee. No jargon. No obligation.