



SME Digital Advisor

Plain-English advice on digital risk

GLOSSARY · CARDS

Glossary Flashcards

Plain-English definitions of IT, cyber and AI terms SME owners encounter.

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

Companion to andrewreaassociates.com

smedigitaladvisor.co.uk

MFA — Multi-Factor Authentication.

A second proof of identity (a code from your phone, a security key) on top of the password. Stops the most common SME breach — stolen-password attacks.

SSO — Single Sign-On.

One login that opens many systems. Reduces password sprawl. Centralises the risk — if SSO is compromised, everything is.

IAM — Identity and Access Management.

The set of tools and rules deciding who can access what.

RBAC — Role-Based Access Control.

People get access based on their job, not their name. Easier to audit.

Privileged access — Admin / superuser rights.

Accounts that can change other accounts, delete data, install software. The keys to the kingdom.

Conditional access — Login rules that depend on context.

“Only allow admin login from inside the office or from a managed laptop.”

OAuth — “Sign in with...” under the bonnet.

How one app gets permission to act on another.

Federated identity — Your identity, used in someone else's system.

Convenient. Means losing your account loses access to many things.

SCIM — Auto-sync of user accounts across SaaS tools.

Creates and disables accounts when HR records change.

Account takeover (ATO) — When an attacker controls a real user account.

Often invisible for days.

Token / session theft — Stealing the “logged-in” cookie, not the password.

Modern attack that bypasses MFA after sign-in.

Ransomware — Malware that encrypts your files and demands a payment.

Modern variants also steal data and threaten to leak it.

Phishing — Fraudulent emails or messages that trick people.

The most common cause of SME breaches.

Spear phishing — Phishing targeted at a specific person.

Researched, personalised. Far more successful than generic phishing.

Whaling — Spear phishing aimed at executives.

Targets directors who can authorise payments.

Smishing — Phishing via SMS / text message.

Often pretends to be a courier, bank, or HMRC.

Vishing — Phishing via phone call.

"This is Microsoft / your bank." Hang up and call back on a known number.

Social engineering — Manipulating a person rather than a system.

Trust and urgency are the levers.

BEC — Business Email Compromise.

Attacker takes over a real email account — usually finance or a director.

Payroll diversion — Fraudster impersonates an employee asking to change bank details.

Verify changes by phone using a number from your records.

Zero-day — A flaw being exploited before there is a fix.

Most real-world breaches use old, well-known flaws on unpatched systems.

Supply-chain attack — Attacking you via one of your suppliers.

Your supplier's problem becomes your problem.

DDoS — Distributed Denial of Service.

Flooding a website with junk traffic until it stops responding.

Drive-by download — Malware that infects you by visiting a website.

Rare with patched browsers but still happens.

Juice jacking — Compromised public USB charging points.

Use your own plug at airports.

USB drop — An attacker leaves an infected USB stick somewhere staff will find it.

Unknown USB sticks go to IT, never into a work machine.

Malware — Malicious software — the umbrella term.

Ransomware, info-stealers, banking trojans, cryptominers.

Info-stealer — Malware whose job is to harvest passwords, cookies, and tokens.

Increasingly common. Why session-token theft bypasses MFA.

RTO — Recovery Time Objective.

How long you can survive being down before it really hurts. Usually shorter than people assume.

RPO — Recovery Point Objective.

How much recent data you can afford to lose. "The last hour" vs "the last day" needs very different backup setups.

3-2-1 backup — Three copies, two media, one off-site.

The minimum rule of thumb.

Immutable backup — A backup that cannot be changed or deleted after writing.

Critical for ransomware survival — the attacker can't encrypt the backups too.

Bare-metal restore — Rebuilding a server from scratch using backup.

Test whether you have this or just file-level backups.

DR / BCP — Disaster Recovery & Business Continuity Planning.

DR is the technical recovery. BCP is keeping the business running while DR happens.

SLA — Service Level Agreement.

What your IT supplier promises to do.

MSP — Managed Service Provider.

Outsourced IT — runs your systems for a monthly fee.

Endpoint — A laptop, desktop, phone, or server.

The place most breaches start.

Patching — Applying security updates.

The single most boring and most effective security activity.

SIEM — Security Information and Event Management.

Collects and watches security logs.

EDR — Endpoint Detection and Response.

Modern antivirus that looks for suspicious behaviour, not just known viruses.

API — Application Programming Interface.

How two systems talk to each other. Treat API keys like passwords.

Webhook — An automated notification one system sends another.

Used by Zapier, Make, Power Automate.

MDM — Mobile Device Management.

Software that lets you enforce passcodes, encryption, and remote wipe on phones and laptops.

SSRF — Server-Side Request Forgery.

Where a website fetches a URL provided by the attacker. OWASP A10.

SBOM — Software Bill of Materials.

A list of every third-party library your application includes.

WAF — Web Application Firewall.

A filter sat in front of your website that blocks common attacks.

CI/CD — Continuous Integration / Continuous Deployment.

The automated pipeline that tests and releases code changes. Without it, changes are made by hand — mistakes are hard to prevent and hard to reverse.

SPF — Sender Policy Framework.

DNS record listing who's allowed to send email from your domain.

DKIM — DomainKeys Identified Mail.

A cryptographic signature on outgoing email.

DMARC — Email authentication policy.

Tells receiving servers what to do when SPF or DKIM fails. Without DMARC at p=reject, criminals can impersonate your domain.

Email spoofing — Forging the “From” field of an email.

Trivially easy without SPF/DKIM/DMARC.

BIMI — Brand Indicators for Message Identification.

Lets your verified logo show next to emails.

GDPR — UK / EU data protection law.

Governs how you handle personal data. Applies to almost every business.

DPA 2018 — Data Protection Act 2018.

The UK domestic law alongside UK GDPR.

Personal data — Information about an identifiable person.

Wider than people think.

ICO — Information Commissioner's Office.

The UK data protection regulator. Breach line: 0303 123 1113.

DPIA — Data Protection Impact Assessment.

A structured review of risk when you do something new with personal data.

DSAR / Subject Access Request — When someone asks for the data you hold on them.

You must respond within one month.

PECR — Privacy and Electronic Communications Regulations.

The cookies + electronic marketing rules.

NIS / NIS 2 — Network and Information Systems Regulations.

Cyber resilience law for “essential” and “important” services. Most SMEs aren't in scope — but you may be if you're a supplier to one.

Cyber Essentials — UK government-backed minimum cyber standard.

Five technical controls. Achievable in weeks.

ISO 27001 — International information-security management standard.

Heavier-weight than Cyber Essentials.

IASME — Cyber-security certification body.

Runs Cyber Essentials assessments.

CIS Controls — A prioritised list of cyber controls.

Free, framework-style.

OWASP — Open Web Application Security Project.

The non-profit behind the OWASP Top 10.

ROPA — Record of Processing Activities.

A list of what personal data you process, why, and for how long. UK GDPR Article 30 requirement for most businesses.

OFSI — Office of Financial Sanctions Implementation.

Part of HM Treasury. Enforces UK sanctions — including the rule that paying ransom to a sanctioned entity is a strict-liability criminal offence.

PCI DSS — Payment Card Industry Data Security Standard.

Applies to any business that takes card payments. Most SMEs comply through their payment processor (e.g. Stripe handles the heavy lifting), but you still have a responsibility for how cards are handled in your business.

EU AI Act — EU regulation on artificial intelligence.

Phasing in 2025–2027. Most SME use of AI is low-risk; high-risk uses (recruitment, credit decisions, healthcare) face stricter rules. Applies to UK firms selling AI services into the EU.

Cyber insurance — Insurance against cyber incidents.

Usually covers ransomware response, business interruption, customer notification.

Deductible / Excess — What you pay before the policy pays.

Set it at a level you could absorb.

Sub-limit — A cap inside a cap.

Your £1m policy may have a £100k sub-limit on social engineering.

Retroactive date — How far back a policy will look.

If you discover a breach today that happened last year, the retroactive date decides whether you're covered.

IR retainer — A pre-paid incident response engagement.

Included with many cyber policies.

LLM — Large Language Model.

The technology behind ChatGPT, Claude, Copilot.

Hallucination — When an AI confidently invents an incorrect answer.

Common, even with good models.

Prompt injection — Hostile instructions hidden in data the AI reads.

A risk for AI that browses, reads emails, or uses tools on your behalf.

Training data — What the AI learned from.

If a vendor “trains on your prompts,” your inputs become part of the model.

RAG — Retrieval-Augmented Generation.

An AI that looks up your documents before answering.

AI agent — An AI that can take actions, not just answer.

Browses the web, runs code, sends emails. Treat agents as junior staff with no probation.

SaaS — Software as a Service.

You log in to use someone else's software.

IaaS — Infrastructure as a Service.

You rent virtual servers.

PaaS — Platform as a Service.

You bring code; the platform runs it.

Shared responsibility model — What the cloud provider does vs what you do.

Cloud providers protect the platform. *You* protect your accounts, data, and configurations. Most cloud breaches are misunderstanding this line — including the fact that Microsoft does not back up your Microsoft 365 data.

Tenant — Your isolated slice of a shared cloud service.

Whoever owns the tenant owns your data.

Data residency — Where your data physically lives.

Matters for GDPR and customer contracts.

VPN — Virtual Private Network.

An encrypted tunnel between two networks.

Firewall — Network filter that allows or blocks traffic.

Still essential.

DNS — The internet's address book.

Who controls your DNS controls your email and website.

TLS / SSL certificate — The padlock in your browser.

Proves the website is who it says it is and encrypts the connection.
Expires — track the date.

Network segmentation — Splitting one network into several.

Stops a compromise in one place spreading.

Zero trust — Don't trust anything by default.

Practical version: MFA everywhere, conditional access, device compliance.

Rate limiting — Capping how often something can be tried.

Stops brute-forcing of logins, password resets, payment attempts.

XSS — Cross-site scripting.

A web flaw that lets an attacker run malicious code in another user's browser.

CSRF — Cross-site request forgery.

Tricking a logged-in user's browser into making a request they didn't intend.