SME Digital Advisor

Plain-English advice on digital risk

GLOSSARY · CARDS

Glossary Flashcards

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

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

Companion to andrewreaassociates.com

smedigitaladvisor.co.uk

GLOSSARY · IDENTITY & ACCESS

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.

GLOSSARY · IDENTITY & ACCESS

SSO — Single Sign-On.

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

GLOSSARY · IDENTITY & ACCESS

IAM — Identity and Access Management.

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

GLOSSARY · IDENTITY & ACCESS

RBAC — Role-Based Access Control.

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

GLOSSARY · IDENTITY & ACCESS

Privileged access — Admin / superuser rights.

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

GLOSSARY · IDENTITY & ACCESS

Conditional access — Login rules that depend on context.

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

GLOSSARY · IDENTITY & ACCESS

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

How one app gets permission to act on another. The scopes you grant matter.

GLOSSARY · IDENTITY & ACCESS

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

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

GLOSSARY · IDENTITY & ACCESS

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

Creates and disables accounts when HR records change.

GLOSSARY · IDENTITY & ACCESS

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

Often invisible for days. MFA + login alerts are the main defences.

GLOSSARY · IDENTITY & ACCESS

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

Modern attack that bypasses MFA after sign-in.

GLOSSARY · THREATS & ATTACKS

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

Modern variants also steal data and threaten to leak it.

GLOSSARY · THREATS & ATTACKS

Phishing — Fraudulent emails or messages that trick people.

The most common cause of SME breaches.

GLOSSARY · THREATS & ATTACKS

Spear phishing — Phishing targeted at a specific person.

Researched, personalised. Far more successful than generic phishing.

GLOSSARY · THREATS & ATTACKS

Whaling — Spear phishing aimed at executives.

Targets directors who can authorise payments.

GLOSSARY · THREATS & ATTACKS

Smishing — Phishing via SMS / text message.

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

GLOSSARY · THREATS & ATTACKS

Vishing — Phishing via phone call.

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

GLOSSARY · THREATS & ATTACKS

Social engineering — Manipulating a person rather than a system.

Trust and urgency are the levers.

GLOSSARY · THREATS & ATTACKS

BEC — Business Email Compromise.

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

GLOSSARY · THREATS & ATTACKS

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

Verify changes by phone using a number from your records.

GLOSSARY · THREATS & ATTACKS

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

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

GLOSSARY · THREATS & ATTACKS

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

Your supplier's problem becomes your problem.

GLOSSARY · THREATS & ATTACKS

DDoS — Distributed Denial of Service.

Flooding a website with junk traffic until it stops responding.

GLOSSARY · THREATS & ATTACKS

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

Rare with patched browsers but still happens.

GLOSSARY · THREATS & ATTACKS

Juice jacking — Compromised public USB charging points.

Use your own plug at airports.

GLOSSARY · THREATS & ATTACKS

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.

GLOSSARY · THREATS & ATTACKS

Malware — Malicious software — the umbrella term.

Ransomware, info-stealers, banking trojans, cryptominers.

GLOSSARY · THREATS & ATTACKS

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

Increasingly common. Why session-token theft bypasses MFA.

GLOSSARY · BACKUP & RECOVERY

RTO — Recovery Time Objective.

How long you can survive being down before it really hurts.

GLOSSARY · BACKUP & RECOVERY

RPO — Recovery Point Objective.

How much recent data you can afford to lose.

GLOSSARY · BACKUP & RECOVERY

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

The minimum rule of thumb.

GLOSSARY · BACKUP & RECOVERY

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

Critical for ransomware survival.

GLOSSARY · BACKUP & RECOVERY

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

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

GLOSSARY · BACKUP & RECOVERY

DR / BCP — Disaster Recovery & Business Continuity Planning.

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

GLOSSARY · OPERATIONS

SLA — Service Level Agreement.

What your IT supplier promises to do.

GLOSSARY · OPERATIONS

MSP — Managed Service Provider.

Outsourced IT — runs your systems for a monthly fee.

GLOSSARY · OPERATIONS

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

The place most breaches start.

GLOSSARY · OPERATIONS

Patching — Applying security updates.

The single most boring and most effective security activity.

GLOSSARY · OPERATIONS

SIEM — Security Information and Event Management.

Collects and watches security logs.

GLOSSARY · OPERATIONS

EDR — Endpoint Detection and Response.

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

GLOSSARY · OPERATIONS

API — Application Programming Interface.

How two systems talk to each other.

GLOSSARY · OPERATIONS

Webhook — An automated notification one system sends another.

Used by Zapier, Make, Power Automate.

GLOSSARY · OPERATIONS

MDM — Mobile Device Management.

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

GLOSSARY · OPERATIONS

SSRF — Server-Side Request Forgery.

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

GLOSSARY · OPERATIONS

SBOM — Software Bill of Materials.

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

GLOSSARY · OPERATIONS

WAF — Web Application Firewall.

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

GLOSSARY · EMAIL SECURITY

SPF — Sender Policy Framework.

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

GLOSSARY · EMAIL SECURITY

DKIM — DomainKeys Identified Mail.

A cryptographic signature on outgoing email.

GLOSSARY · EMAIL SECURITY

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.

GLOSSARY · EMAIL SECURITY

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

Trivially easy without SPF/DKIM/DMARC.

GLOSSARY · EMAIL SECURITY

BIMI — Brand Indicators for Message Identification.

Lets your verified logo show next to emails.

GLOSSARY · DATA & COMPLIANCE

GDPR — UK / EU data protection law.

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

GLOSSARY · DATA & COMPLIANCE

DPA 2018 — Data Protection Act 2018.

The UK domestic law alongside UK GDPR.

GLOSSARY · DATA & COMPLIANCE

Personal data — Information about an identifiable person.

Wider than people think — includes business contact details.

GLOSSARY · DATA & COMPLIANCE

ICO — Information Commissioner's Office.

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

GLOSSARY · DATA & COMPLIANCE

DPIA — Data Protection Impact Assessment.

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

GLOSSARY · DATA & COMPLIANCE

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

You must respond within one month.

GLOSSARY · DATA & COMPLIANCE

PECR — Privacy and Electronic Communications Regulations.

The cookies + electronic marketing rules.

GLOSSARY · DATA & COMPLIANCE

NIS / NIS 2 — Network and Information Systems Regulations.

Cyber resilience law for “essential” and “important” services.

GLOSSARY · DATA & COMPLIANCE

Cyber Essentials — UK government-backed minimum cyber standard.

Five technical controls. Achievable in weeks.

GLOSSARY · DATA & COMPLIANCE

ISO 27001 — International information-security management standard.

Heavier-weight than Cyber Essentials.

GLOSSARY · DATA & COMPLIANCE

IASME — Cyber-security certification body.

Runs Cyber Essentials assessments.

GLOSSARY · DATA & COMPLIANCE

CIS Controls — A prioritised list of cyber controls.

Free, framework-style.

GLOSSARY · DATA & COMPLIANCE

OWASP — Open Web Application Security Project.

The non-profit behind the OWASP Top 10.

GLOSSARY · DATA & COMPLIANCE

ROPA — Record of Processing Activities.

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

GLOSSARY · INSURANCE

Cyber insurance — Insurance against cyber incidents.

Usually covers ransomware response, business interruption, customer notification.

GLOSSARY · INSURANCE

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

Set it at a level you could absorb.

GLOSSARY · INSURANCE

Sub-limit — A cap inside a cap.

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

GLOSSARY · INSURANCE

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.

GLOSSARY · INSURANCE

IR retainer — A pre-paid incident response engagement.

Included with many cyber policies.

GLOSSARY · AI

LLM — Large Language Model.

The technology behind ChatGPT, Claude, Copilot.

GLOSSARY · AI

Hallucination — When an AI confidently invents an incorrect answer.

Common, even with good models.

GLOSSARY · AI

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

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

GLOSSARY · AI

Training data — What the AI learned from.

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

GLOSSARY · AI

RAG — Retrieval-Augmented Generation.

An AI that looks up your documents before answering.

GLOSSARY · AI

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

Treat agents as junior staff with no probation.

GLOSSARY · CLOUD

SaaS — Software as a Service.

You log in to use someone else's software.

GLOSSARY · CLOUD

IaaS — Infrastructure as a Service.

You rent virtual servers.

GLOSSARY · CLOUD

PaaS — Platform as a Service.

You bring code; the platform runs it.

GLOSSARY · CLOUD

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

Most cloud breaches are misunderstanding this line.

GLOSSARY · CLOUD

Tenant — Your isolated slice of a shared cloud service.

Whoever owns the tenant owns your data.

GLOSSARY · CLOUD

Data residency — Where your data physically lives.

Matters for GDPR and customer contracts.

GLOSSARY · NETWORK & WEB

VPN — Virtual Private Network.

An encrypted tunnel between two networks.

GLOSSARY · NETWORK & WEB

Firewall — Network filter that allows or blocks traffic.

Still essential.

GLOSSARY · NETWORK & WEB

DNS — The internet's address book.

Who controls your DNS controls your email and website.

GLOSSARY · NETWORK & WEB

TLS / SSL certificate — The padlock in your browser.

Expires — track the date.

GLOSSARY · NETWORK & WEB

Network segmentation — Splitting one network into several.

Stops a compromise in one place spreading.

GLOSSARY · NETWORK & WEB

Zero trust — Don't trust anything by default.

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

GLOSSARY · NETWORK & WEB

Rate limiting — Capping how often something can be tried.

Stops brute-forcing of logins.

GLOSSARY · NETWORK & WEB

XSS — Cross-site scripting.

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

GLOSSARY · NETWORK & WEB

CSRF — Cross-site request forgery.

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