FREE GUIDE

The Plain-English Security Dictionary

Every security term you'll meet as a small-business owner — explained the way a person would actually say it.

Security has a vocabulary problem. The ideas are mostly simple; the words are not. This dictionary translates the terms you'll meet — in vendor pitches, insurance forms, customer questionnaires, and the news — into plain English, with a line on why each one matters to a small business. Keep it open next to anything security-related you have to read.

A free guide from Sylvan Assurance — plain-English security, without us ever seeing your data.

Sylvan Press · Sylvan Assurance, LLC · Copyright 2026

Signing in

Two-step login (MFA, 2FA, multi-factor authentication). A second step when you sign in — a code or a tap on your phone — in addition to your password. It means a stolen password alone isn't enough to get into your account. If you adopt one habit from this whole dictionary, this is the one.

Password app (password manager). An app that creates and remembers strong, different passwords for every account, so you don't have to. Reusing one password everywhere means one leaked site exposes all of them; a password app removes that risk.

Login details (credentials). Your username and password — and anything else that proves it's you. When the news says credentials "leaked," it means lists of usernames and passwords are circulating.

Authentication. The formal word for proving it's you when you sign in. Passwords, codes, fingerprints — all authentication.

Access control (authorisation). Deciding who can get into what. Good access control means people have only the access their job needs — so one compromised account can't reach everything.

Least privilege. The rule behind good access control: give people only the access they need, nothing extra. It limits how much damage any single mistake or stolen login can do.

Scams and attacks

Phishing (fake messages). A message designed to trick you — usually into clicking a link, opening a file, or "confirming" your login details. Still the most common way small businesses get breached, because it works on people, not technology.

Social engineering. The broader family of scams that trick people rather than break technology — fake invoices, urgent calls "from the bank," a "CEO" emailing for gift cards. The defence is a pause-and-verify habit, not software.

Business email compromise (BEC). A scam where an attacker gets into (or convincingly fakes) a business email account and uses it to redirect payments or invoices. One of the most expensive scams for small businesses.

Ransomware. Software that locks your files and demands payment to unlock them. The honest defence isn't avoiding it perfectly — it's having backups good enough that you can refuse to pay.

Vulnerability. A known weak spot in software that attackers can use. Vendors fix these with updates — which is why "keep things updated" appears on every security list ever written.

Attacker (threat actor). Whoever's on the other side — a person or a program. Most small businesses aren't targeted personally; they're caught by attacks fired at thousands of businesses at once. Being a slightly harder target than average is genuinely effective.

Your devices and software

Device (endpoint). Any computer, phone, or tablet that touches your business. Security paperwork says "endpoint"; it means your laptop.

Keeping things updated (patching, patch management). Installing software updates promptly — they're mostly fixes for known weak spots, not just new features. "Patch management" simply means having a routine for it instead of doing it when you remember.

Firewall. A filter that blocks unwanted network connections to your systems. Your office router and your computer almost certainly have one — the practical question is whether it's turned on.

Secure connection (VPN, virtual private network). An encrypted link between your device and another network, useful on hotel and café Wi-Fi. One caution: a VPN protects data in transit; it doesn't make a device "secure" by itself, whatever the ads say.

Encryption. Scrambling data so only someone with the key can read it. Modern phones and laptops can encrypt everything they store — usually one switch in settings — so a lost device is an inconvenience instead of a breach.

Backups and recovery

Backup. A spare copy of your important data, kept somewhere a problem with the original can't reach — including ransomware, which is why at least one copy should be separate from your main systems, with its own login.

Restore test. Actually trying to bring files back from a backup. An untested backup is a hope, not a plan; many businesses discover theirs was broken at the worst possible moment.

Disaster recovery (DR). The plan for getting back to work after something big — fire, flood, ransomware, the laptop with everything on it dying. For a small business this can be one page: what we restore first, who does it, where the backups live.

Recovery time. How long you can actually afford to be down — knowing it tells you how good your backup arrangements need to be. A day? A week? The honest answer often surprises owners.

When something goes wrong

Breach (incident). When something actually happens — an account taken over, data exposed, files locked. The formal word is "incident"; either way the first hour of your response matters more than most people expect.

Incident response (IR). What you do when it happens: a short, written plan of who does what, in what order, so decisions get made calmly instead of invented under pressure.

The 72-hour clock. Under the EU's data-protection law (the General Data Protection Regulation, GDPR), certain personal-data breaches must be reported to a regulator within 72 hours of becoming aware. If you hold data about people in Europe, this clock is worth knowing about before you ever need it.

Notification. Formally telling the people affected — regulators, customers, sometimes insurers — about a breach. What you must send, and when, depends on the rules that apply to you; templates prepared in advance make this far less painful.

Security questionnaire (SIG, CAIQ, vendor assessment). A long form a bigger customer sends before buying from you, asking how you handle security — the common named ones are the Standardized Information Gathering questionnaire (SIG) and the Consensus Assessments Initiative Questionnaire (CAIQ). Increasingly the toll booth between a small vendor and a big deal — annoying, but answerable with honest preparation.

Where to go from here

Most of the terms above show up in one of our free assessments — short, plain-English, and they run entirely in your browser, so we never see your answers. The SMB Security Assessment is the best place to start.

When you're ready to turn a score into a plan with the templates to carry it out, the Full Edition lays it all out — from $49, one-time, with a 30-day money-back guarantee.

Take the free assessment: sylvanassurance.com/free/smb-security/

See the Full Edition: sylvanassurance.com/smb-security-assessment.html

Scan for the free assessment that goes with this guide.
sylvanassurance.com/go/free-smb-security-assessment

This guide provides general guidance and recommended security practices drawn from widely recognised standards. It is not a professional security audit and not legal advice, and it does not guarantee security or prevent any particular breach. Responsibility for your business's security remains with you. © 2026 Sylvan Assurance, LLC.