



ASCENDEA

AI / BUSINESS GROWTH / EBOOK & PLANNING WORKSHEETS

Practical Online Business Security for UK SMEs

A plain-English, UK-focused guide for small-business owners and managers to strengthen accounts, websites, online payments, customer data, backups and scam response. It includes step-by-step actions, role-based SOPs, standalone checklists and a 30-day implementation plan; it does not provide certification or a compliance guarantee.



Author: Rob Arnold

ascendea.ai

ASCENDEA EDITION · OCTOBER 2026 · v1.0

Free Ascendea resource

Your route through this resource

Publication and permitted-use notice	3
How to use this guide	4
Start with a simple security map.....	4
Secure accounts before buying more tools	7
Keep websites, online shops and payments in scope	10
Secure the devices and network that reach your services	12
Protect customer, staff and business information	13
Make it hard for scams to work.....	16
Build backups and recovery you can actually use	19
Respond to an incident calmly and in order	22
Build a security toolkit that fits the business	24
A realistic 30-day implementation plan	26
Make security a routine, not a once-only project	30
Standalone checklists.....	33
Your security action workbook	34
Official resources and source notes	36

Chapter links and PDF bookmarks support navigation. Writing areas are for handwritten or separate notes, not interactive PDF forms.

Author: Rob Arnold · Ascendea · Edition v1.0 · October 2026

<https://ascendea.ai/>

Educational guidance; not a guarantee of business results or legal, tax or personalised financial advice. This is a non-exclusive licensed-content adaptation. For your own learning and permitted end use only; no resale, redistribution, editable-source or private-label rights are granted.

A plain-English guide, working checklists and 30-day action plan

Author: Rob Arnold · Ascendea · ascendea.ai

Edition v1.0 · October 2026

This guide is for UK small-business owners and managers who use email, cloud files, websites, online payments or customer records. It turns everyday security into clear working practices. You do not need to be technical to use it, but you do need to decide who owns each action and follow through.

General education only. This guide is not legal, data-protection, insurance, payment-card, IT-security or professional advice. Security controls reduce risk; they do not guarantee that an incident will not happen or that a business is compliant. Check current official guidance and your providers' documentation, and obtain qualified help where the risk, contract or regulation requires it.

Publication and permitted-use notice

Author of this Ascendea edition: **Rob Arnold**. Publisher: **Ascendea**. Website: <https://ascendea.ai/>.

This Ascendea edition is a non-exclusive licensed adaptation of private source material, rebuilt with UK-focused guidance, current primary sources, operational checklists and beginner-friendly procedures. The source-acquisition proof records the licensed Entrepedia account, native source ZIP and published PLR rebrand/giveaway permissions for this permitted UK SME use. It does not claim exclusive ownership of the underlying licensed base material. This finished edition is available as a free Ascendea resource.

Provided for your own learning and permitted end use. **No resale, redistribution, private-label, editable-source or source/PLR rights are granted.** Do not copy this resource into a product for others or present it as security certification.

How to use this guide

Start with the 15-minute triage checklist, then complete the 30-day plan. Do not buy a long list of products before the basics work. A password manager, multi-factor authentication (MFA), updates, a tested backup and a clear route for reporting suspicious activity are more useful than an expensive tool nobody uses.

Treat the worksheets as a working record. Write down the accounts, data and processes your business depends on; name an owner; and set the next review date. If you are a sole trader, one person can fill several roles. If you have a team, do not assume the business owner is the only person who needs to know the process.

The fictional examples in this guide are teaching examples. They are not Ascendea client stories, endorsements or results. Any timing, budget or tool tier is illustrative rather than a promise or market benchmark.

What good enough looks like this month

You are aiming for a defensible starting point, not perfection:

- Important accounts have their own logins, strong unique passwords and MFA where available.
- Nobody shares passwords by email, chat or sticky note; necessary shared access is controlled and recorded.
- Devices, browsers, website software and extensions are supported and updated.
- You know what personal and business-critical data you hold, where it lives and who can access it.
- You can restore a meaningful sample of backed-up data.
- Your team knows how to pause, verify and report a suspicious request.
- You have an incident contact list and a written first-response procedure.

The UK National Cyber Security Centre (NCSC) frames security for small organisations around protecting accounts and devices, spotting scams and making usable backups. Its current small-organisation guidance is a useful companion to this guide.^[^ncsc-small]

Start with a simple security map

Security is easier when you can see what needs protecting. Make a first-pass map in one meeting. You are not trying to catalogue every spreadsheet; you are identifying systems whose loss, misuse or unavailability would seriously interrupt the business.

List the things that matter

Use the table below for the first version. Include supplier-managed services, not just equipment you own. For a small electrical contractor, this might include the shared inbox, quoting software, accounting system, job photos, cloud drive, website, payment terminal and director's phone. For a professional-services firm, it may include case files, document signing, client portal, payroll and the office Wi-Fi.

Asset or service	What it supports	Information involved	Main owner	Who has admin access?	If unavailable or misused, what happens?	Next action
Business email	Enquiries, password resets, invoices	Customer and supplier contact data				
Website / online shop	Public information, enquiries, orders	Visitor details, forms, order data				
Payment provider	Card payments / refunds	Transaction data; do not record card details locally				
Cloud file storage	Contracts, quotes, staff files	Commercial and possibly personal data				
Accounting / payroll	Invoicing and pay	Financial and personal data				
Devices and mobile phones	Access to every service above	Credentials, files, messages				

Choose the first five actions

For each row, ask four plain questions:

1. **What could go wrong?** Examples include a lost phone, a reused password, an ex-employee account, an unpatched website extension, a fake invoice, or an accidental public-sharing link.
2. **How would we notice?** Decide whether an owner sees an alert, a customer reports it, a bank query arrives, or nobody would know.
3. **What limits the damage?** A separate login, MFA, least-privilege access, a payment callback, a backup or a manual fallback can each help.
4. **Who will make the change by when?** A control without an owner is only an intention.

Prioritise an issue when it affects your email, banking, payments, website administration, customer database, business-wide files or a director/administrator account. A low-cost change that reduces access to a high-impact system normally goes ahead before a complicated new security product.

Assign responsibility without creating a bottleneck

One person should own the security calendar. That does **not** mean they must be able to see every record or carry out every technical task. Use a small split of duties:

Role	Typical responsibility	Do not assume this role can also do
Business owner / director	Budget, risk decisions, supplier escalation	Daily monitoring or technical recovery alone
System owner	Knows how a service is used; approves access	Legal breach decisions or payment release alone
Administrator	Adds/removes accounts; maintains records	Access to every customer file by default
Finance approver	Independently verifies payment changes	Sole authorisation of urgent or unusual payments
Staff member / contractor	Uses services and reports concerns	Admin rights just to complete normal work

A two-person check is especially valuable where changing bank details, issuing refunds, adding a payment-user account or recovering a privileged account could cause a loss.

Secure accounts before buying more tools

An account is a doorway into systems and data. Email deserves special attention because it is often used to reset passwords for other services. Website, payment-provider, cloud-storage, accounting, social-media and domain/DNS accounts also need deliberate protection.

Use individual accounts and a password manager

Give each person their own account wherever the service allows it. A named account makes it possible to remove access when a person leaves and to investigate unusual activity. Avoid a generic admin@, sales@ or shared website login used by several people. A shared mailbox can still receive messages while individual users sign in with their own accounts.

A reputable password manager can generate and store a different long password for each service. It reduces the temptation to reuse a memorable password or keep passwords in a document. The NCSC says the security benefits normally outweigh the risks, but selection and recovery arrangements still matter.^[^ncsc-password-manager]

Set it up step by step:

1. Choose a business-capable product that works on the devices and browsers your team actually uses. Check how it encrypts stored credentials, handles MFA, applies updates, provides audit records and supports removal of a leaver. Do not choose solely from an advert or price comparison.
2. Create the business account using a named owner and a business-controlled recovery email. Enable MFA on the password-manager account before importing anything.
3. Make a separate vault or shared collection only for credentials that genuinely must be shared. Prefer delegated access or individual roles in the underlying service over sharing a password.
4. Add the highest-risk accounts first: primary email, domain/DNS, hosting, website administrator, payment provider, bank, accounting, cloud administrator and social-media administrator.
5. Change each imported high-risk password to a newly generated unique value. Do not simply copy old passwords into a new tool.
6. Record who administers the password manager and how account recovery works. Test the approved recovery route in a planned session, not during an emergency.
7. Invite colleagues one at a time. Show them how to use the correct work vault, how to unlock it securely and how to report a suspected fake website.
8. Review access after a staff change and at least on the monthly schedule in this guide.

Never ask staff to send a master password or MFA code to a manager. A recovery process that lets any administrator silently read every personal vault creates a significant risk. Decide what recovery is necessary and understand who can use it.

Turn on MFA, passkeys or a stronger sign-in method

MFA asks for more than one factor to sign in. It can reduce the impact of a stolen password, but it is not a reason to reuse passwords or approve unexpected sign-in prompts. Where a service offers passkeys or phishing-resistant methods, assess whether they work for your team and recovery process. Where an authenticator app, hardware security key or app prompt is used, enrol a managed backup method before relying on it.

Begin with this order:

1. Primary business email and its administrator account.
2. Password-manager vaults.
3. Domain registrar and DNS host.
4. Banking, accounting and payment-provider accounts.
5. Website hosting, administrator accounts and e-commerce administration.
6. Cloud storage, CRM, payroll, remote access, social media and other services holding business data.

For each account, record the user, method, recovery owner and last test date. Store recovery codes in the approved password-manager item or another controlled secure location; do not leave them in an inbox or phone photo album. If a provider offers only SMS codes, use them rather than no MFA while you review stronger available options. Protect the phone account and make sure a second authorised person can continue business operations if the primary phone is unavailable.

Give the least access needed

Least privilege means a person receives only the access needed for their current work. It is a practical damage-limitation measure, not a sign that you distrust staff.

Task	Usually sufficient access	Access usually not needed
Writer updating articles	Website editor / contributor role	Website owner, hosting or payment settings
Retail colleague packing orders	Order fulfilment view and shipping actions	Export of all customers or refund administration
Bookkeeper reconciling invoices	Accounting role appropriate to the job	Bank administrator or website super-admin
Web developer fixing a feature	Time-limited staging or specified production role	Primary email, payment-provider owner or customer database export

Task	Usually sufficient access	Access usually not needed
Marketing contractor scheduling posts	Named social-media role	Passwords for all platforms or business bank access

Create roles in the service rather than sharing an owner account. Keep a small access register containing the service, account owner, access level, approver, start date, expected end date and review date. Also review connected apps: a tool you trialled last year may still have permission to read a mailbox, access files or post on your behalf.

Onboard and offboard safely

At onboarding, provide the account only after the manager confirms the person's job need. Require MFA, give a short security briefing and show the reporting route. At offboarding, time matters. Disable or remove access on or before the agreed final date, remove group membership and active sessions where available, collect business devices, transfer ownership of work files and change any shared credentials the person could still use. Check SaaS apps, payment systems, website users, VPN/remote access, shared folders and social-media roles, not only email.

A planned contractor end date is a useful trigger for temporary access. If the work is extended, renew the approval rather than allowing access to drift on indefinitely.

Account-security checklist

Use this standalone list for the first account clean-up.

- ☐ I have named the owner of email, domain/DNS, website, payment, cloud files and accounting.
- ☐ Each person uses a named account; shared accounts are being removed or strictly controlled.
- ☐ A password manager protects the critical accounts, and its own MFA is enabled.
- ☐ High-risk accounts have unique generated passwords and MFA or an approved stronger sign-in method.
- ☐ Recovery codes and recovery contacts are documented in a controlled place.
- ☐ Website, cloud, payment and social-media admin roles have been reviewed.
- ☐ Old staff, contractor and trial-app access has been removed.
- ☐ A manager can complete the onboarding/offboarding SOP in this guide.

Keep websites, online shops and payments in scope

A public website is part of the business attack surface even if it only contains a contact form. An online shop, customer portal or booking system deserves additional attention because it may process orders, collect personal data or integrate with a payment provider.

Understand what HTTPS does — and does not — do

A website using `https://` uses TLS to protect data in transit between the visitor and the site. The browser may show a lock icon. This is important, but it is not proof that a website is trustworthy, free of malware or compliant with every privacy and payment obligation. Attackers can also use HTTPS.

Check that every public page redirects to HTTPS and that there are no browser certificate warnings. Your web host, platform or developer can help if this is unfamiliar. Do not ask a customer to ignore a browser security warning. Treat it as a reason to pause and investigate.

Update carefully, not blindly

Unpatched software can contain known flaws. The NCSC recommends keeping operating systems, browsers, extensions, third-party apps and security software supported and up to date; automatic updates should be enabled where possible and checked because they can fail.^[^ncsc-updates]

For a website, apply the same principle without unnecessarily risking a live shop:

1. Make or confirm a current backup of the site, database and configuration. Know where the backup is and how a restore would be requested.
2. Record the current version, key plugins/extensions and the person responsible.
3. Read the update notice. For a high-impact platform or a complex site, ask the developer or host whether it needs staging/testing first.
4. Update the platform, theme/template and extensions from trusted, official sources. Remove extensions you no longer need rather than keeping disabled abandoned code.
5. Test the public site, contact form, login, basket/checkout, emails and critical integrations after the change. Use a non-production test order where the platform supports it.
6. If something breaks, use the documented rollback or seek provider/developer support. Do not keep a known-vulnerable version indefinitely because the update was inconvenient.

Choose a host or website platform by asking about support, patching responsibility, backups, restoration options, MFA, user roles, incident contact route, logging, DDoS protection where relevant and how security notices reach you. Features, packages, pricing and responsibilities change, so verify them in the current contract and documentation rather than relying on a generic provider list.

Keep website administration separate from everyday browsing

Use named accounts and MFA for hosting, CMS and e-commerce administration. Do admin work from a supported device, not a borrowed public computer. Do not install a plugin or paste a code snippet because a forum post says it will improve speed or sales. First identify the publisher, purpose, permissions, update history, compatibility and rollback method. Limit administrator accounts and remove developer access when a project ends.

Set up basic monitoring that tells an owner when the site is unavailable, a certificate is about to expire or a security provider detects a problem. Monitoring does not replace a response plan. Agree who receives the alert outside ordinary hours and what action they are authorised to take.

Use a payment provider to reduce unnecessary card-data handling

PCI DSS is intended for entities involved in payment processing, regardless of merchant size. The precise validation and reporting expectations depend on the acquirer/merchant bank or payment brand, and the applicable Self-Assessment Questionnaire depends on the payment setup.^[^pci-merchants]

For many small online businesses, a reputable payment provider's hosted checkout, redirect or documented embedded payment component can reduce the card-data environment you manage. It does **not** automatically make your whole business PCI compliant or remove the need to check the arrangement with your acquirer and provider.

Practical payment rules:

- Do not request or retain full card numbers, magnetic-stripe data or card-security codes in email, chat, forms, spreadsheets, paper notes or your own website database unless a properly scoped, specialist-approved arrangement requires it.
- PCI DSS does not permit retaining card verification codes after authorisation, even if a customer asks you to do so.^[^pci-cvv]
- Use the payment provider's tokenised customer/payment method or recurring-payment feature where appropriate instead of copying card details into your records.
- Keep the payment-provider owner account separate from ordinary order-fulfilment access. Use named staff accounts and remove leavers quickly.
- Confirm who can issue refunds, change bank details, alter settlement settings or add users. Require independent verification for unusual refunds or settlement changes.
- Keep software and integrations that affect checkout supported and updated. Ask the provider and acquirer which security notices, scans or validation activities apply to your payment flow.
- If you receive card details by email or another unsuitable channel, do not forward or reply quoting the data. Follow your provider's documented process, minimise exposure and ask the customer to use the approved payment route.

Physical retailers should also keep an inventory of card terminals, know what each terminal normally looks like and report suspected tampering promptly to the terminal provider or acquirer. Do not allow an unexpected caller or visitor to service a terminal without independent verification.

Review suspicious orders fairly

Fraud controls should identify a reason to check an order, not become a reason to make unfair assumptions about a customer. Use the provider's available fraud signals, delivery confirmation, clear returns terms and a documented manual-review step. Examples that may warrant a check include a sudden unusually high-value order, repeated failed payment attempts, contradictory delivery information or a request to change delivery after payment. Verify through an established route and avoid asking for more personal data than is necessary.

Document the reason for a cancellation or hold. If a customer disputes a transaction, preserve the relevant permitted order, delivery and communication records and follow the payment provider's chargeback/dispute procedure.

Website and payment checklist

- ☐ All public pages use HTTPS without certificate warnings.
- ☐ I know who owns the domain, DNS, host, CMS and e-commerce administration.
- ☐ Admin accounts use named logins, unique passwords and MFA where available.
- ☐ Website platform, template and extensions are supported, necessary and updated through a documented process.
- ☐ A backup and rollback/support route exists before material site changes.
- ☐ The checkout uses the payment provider's approved integration; no card details are kept in ordinary business systems.
- ☐ Payment roles, refund limits and bank-detail change checks are documented.
- ☐ The acquirer/provider has confirmed the current PCI DSS validation route that applies to our setup.
- ☐ Someone receives and can act on website/security alerts.

Secure the devices and network that reach your services

A well-protected account can still be exposed by a compromised laptop or phone. Include Windows, Mac, mobile devices, tablets, browser extensions and home-working equipment in the security map.

Minimum device practices

1. **Use a screen lock.** Set a device PIN/password or approved biometric lock and configure a reasonable automatic lock time.
2. **Keep support current.** Replace or isolate devices and operating systems that no longer receive security updates. An old device may be cheaper to keep than replace, but it can create an unmanaged route into business accounts.
3. **Enable updates.** Turn on automatic operating-system, browser and app updates where compatible. Reboot when required and check occasionally that updates are actually completing.
4. **Limit administrator rights.** Everyday users normally should not install software or browser extensions without a business need and approval.
5. **Protect lost devices.** Turn on provider-supported device location/remote-lock or wipe features when proportionate. Record how to use them before a device goes missing.
6. **Separate guest access.** Change the default router administrator password; use current router security settings; keep guest Wi-Fi separate from business devices where practical. Ask a trusted IT supplier for help if you do not know how to configure the router safely.
7. **Agree a bring-your-own-device (BYOD) boundary.** State whether personal devices may access business email or files, the minimum update/lock requirements and what happens when the working relationship ends.

Do not assume that private/incognito browsing protects the device, hides activity from every party or removes the need for updates. It has a narrower purpose.

A fictional example: a small firm avoids a large clean-up

Fictional example. A three-person surveying practice uses a shared email address, one website administrator login and a director's personal mobile for all recovery codes. In its first security review, the practice creates named email and website accounts, moves passwords into a controlled vault, gives the office manager a limited website-editor role and records a backup recovery contact. Nothing dramatic happens that week. The improvement is that one accidental click or a staff departure is less likely to give uncontrolled access to every system at once.

Protect customer, staff and business information

Cyber security and data protection overlap, but they are not the same thing. Security is about preventing and managing unauthorised access, loss, alteration or unavailability. Data protection is also about why you use personal data, how much you use, who you tell, how long you keep it and how you respect people's rights.

Personal data can include a customer name and email, a staff record, an enquiry form, an IP address in context, a recorded call or a job photograph that identifies someone. It is not limited to a customer database.

Make a practical data inventory

Before changing policies, list the information you hold and why. A small business may find that most data sits across its email, cloud drive, accounting system, website forms, CRM, booking system, marketing platform and devices rather than one central database.

Information set	Purpose	Where held	Who can access it	Supplier / processor	Retention or review point	Risk or action
Customer enquiry forms	Answer requests and quote	Website / email				
Job / project files	Deliver contracted work	Cloud drive				
Invoices and payments	Accounting and tax records	Accounting provider				
Staff records	Employment administration	Restricted HR folder				
Marketing contacts	Send chosen communications	CRM / email platform				

The ICO describes data minimisation as keeping personal data adequate, relevant and limited to what is necessary for the stated purpose. It advises organisations to review data periodically and delete what is no longer needed.^[^ico-minimisation] Do not collect a date of birth, identity document, health detail or personal contact channel merely because a form field is available.

Improve access and file sharing

Classify information in a way your team can use. For many SMEs, **public**, **internal** and **restricted** are enough. Define them in one sentence each. For example, a published price list is public; a draft service procedure may be internal; client files, staff records, supplier bank details and credentials are restricted.

Use your cloud service's named-user permissions, groups and folders. Share a specific folder with a specific person for a defined purpose rather than emailing a copy to everyone or setting a broad public link. Review shared links, external guests and download permissions. Where a provider offers expiry dates, passwords or audit logs, decide whether they are appropriate for your use case and configure them deliberately.

Cloud storage is not automatically safer or less safe than a local computer. The practical questions are whether the account has MFA, access is controlled, provider responsibilities are understood, devices are protected, data can be recovered and the service fits your business process. Choose a provider on current documented features, contractual needs, support, data location/transfer questions where relevant and how well staff can use it securely. Do not treat a generic product comparison as assurance.

Create a privacy notice that matches reality

Your privacy notice should describe what you actually do, not copy a policy from an unrelated website. Explain in plain language:

- what categories of personal data you collect;
- the purposes and relevant lawful basis for each use;
- who receives the information, such as a payment, payroll, delivery, CRM or IT provider;
- any relevant international-transfer information;
- how long you keep information or the criteria used to decide;
- people's rights and how to contact you or make a complaint; and
- any automated decision-making that has the relevant legal effect or similarly significant effect.

Update the notice when a material processing activity changes. A privacy notice is not a substitute for making the underlying processing fair, lawful, secure and proportionate. Use the ICO's current small-business tools and guidance for your circumstances; its guidance is under review following legal changes, so recheck it before relying on an old template.^[^ico-minimisation]

Customer contact and B2B outreach: do not mix up company types

This resource is not a direct-marketing playbook, but security teams often inherit contact lists and email systems. If you use business contact details to send promotional email, get current advice before launching a campaign.

Under the ICO's current B2B guidance, companies and LLPs are generally **corporate subscribers** for PECR purposes. Sole traders and certain ordinary partnerships are **individual subscribers**, which have greater protections. The PECR electronic-mail rule does not apply to corporate subscribers in the same way, but marketers must not hide their identity, must provide a valid opt-out address and should honour opt-outs. UK GDPR still applies when you process identifiable business contact data: you need an appropriate lawful basis and privacy information.^[^ico-b2b]

Do not assume a visible work email address is blanket permission to send marketing. Do not assume that a sole trader is safe to treat like a limited company. Keep a suppression list, record the source of contacts and stop when someone objects. The ICO flags this area as under review; verify the current rules and seek specialist advice for a real campaign.[^ico-b2b]

Know what a personal-data breach means

A personal-data breach is not only a hacker stealing a database. It can include an unauthorised disclosure, access, loss, alteration, destruction or significant loss of availability of personal data. Examples include sending a client spreadsheet to the wrong recipient, losing an unencrypted device, exposing a folder through a public link or a provider notifying you of unauthorised access.[^ico-breach]

If an incident occurs, contain it and assess the risk to affected people. Where a personal-data breach is likely to create a risk to people's rights and freedoms, the controller must notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware. If the risk is high, affected individuals must be informed without undue delay. Not every incident is reportable, but document every breach, your facts, risk assessment, decision and remedial action.[^ico-breach]

This is a case-specific legal assessment. Do not delay containment while debating legal terms, and do not tell customers there was "no impact" before the facts are known. Your processor contracts should require a provider to tell you promptly when it becomes aware of a relevant breach, enabling the controller to assess notification obligations.[^ico-breach]

Data-protection checklist

- ☐ We have a usable data inventory covering website forms, email, cloud storage, finance, CRM, staff information and suppliers.
- ☐ We collect only data we can explain as necessary for a clear purpose.
- ☐ Restricted folders, shared links and external guests have been reviewed.
- ☐ Each system has a named owner and appropriate named-user access.
- ☐ Our privacy notice describes our actual data uses, suppliers, retention approach and contact route.
- ☐ We have a process for rights requests and a breach log.
- ☐ Processor/supplier contracts and breach-contact routes have been identified where relevant.
- ☐ Marketing contacts are segmented by type of subscriber and screened against opt-outs.

Make it hard for scams to work

Many incidents begin with a message, a call or a request that looks plausible. The goal is not to train people to spot every scam by intuition. It is to build working processes that make unsafe actions difficult to complete.

The NCSC advises a layered approach to phishing: suitable email filtering, support for staff to identify and report suspicious messages, controls that reduce the impact of a click, and rehearsed incident response.^[^ncsc-phishing]

Recognise the request — then verify independently

A suspicious message may be well written, use your supplier's branding or appear in an existing email thread. Poor spelling is not a dependable test. Treat these as reasons to pause:

- a request for a password, MFA code, recovery code or remote access;
- pressure to bypass a normal process, secrecy or an artificial deadline;
- a supplier request to change bank details, payment method or delivery address;
- a request to approve an unexpected invoice, refund or gift-card purchase;
- an unexpected attachment, sign-in link or document-sharing invitation;
- a call claiming to be IT support, a bank, a director or a provider that asks you to act immediately; or
- a message asking you to disclose customer, staff or business data.

Do not use the contact details, link or reply button supplied in the suspicious message to verify it. Use a number already held in your records, a known supplier portal, a bookmarked official website or an established colleague channel. For a payment change, use a known telephone number and ask a known contact to confirm a detail that was not provided by the requester.

AI can make impersonation, voice and image content more convincing. That changes neither the rule nor the fallback: a familiar voice, logo or writing style is not payment authority. Use the independent verification process.

Put payment-change verification in writing

A useful payment process does not depend on one rushed person making a perfect judgement. Document:

Event	Minimum check	Who may complete it	Evidence to keep
New supplier bank details	Call verified known contact on existing number; confirm change and relevant reference	Finance owner plus independent approver	Date, number source, person, outcome
Urgent payment request	Confirm underlying order/ contract and approval route	Authorised approver	Request, approval, exception reason

Event	Minimum check	Who may complete it	Evidence to keep
Refund above normal threshold	Review order, payment-provider record and reason	Different person where practical	Order ID, decision, reviewer
New payment-user invitation	Check job need and grant lowest role	System owner	Access-register entry

A verbal confirmation should be recorded, but do not record unnecessary secrets or full payment-card details. If a caller will not allow verification, treat that as a reason not to proceed.

Encourage reporting, not blame

Staff need permission to say, “I am going to verify this through our normal route.” Make reporting simple: for example, a named mailbox, service-desk route or team channel that the owner monitors. Make it clear that a person who reports a suspicious message or a mistaken click promptly is helping the business. The NCSC warns that blame-oriented cultures reduce timely reporting.^[^ncsc-phishing]

Brief, practical refreshers work better than an annual lecture that nobody remembers. In a monthly or quarterly meeting, show one recent scam pattern, repeat the payment-change rule, confirm the reporting route and update the contact list. Do not send harmful live examples to staff or run punitive simulations without considering the effect on trust and workload.

SOP: suspected phishing, impersonation or malicious link

Field	Procedure
Owner	Security coordinator; system owner takes account-specific action
Trigger / input	Suspicious email, text, call, attachment, login prompt or reported click
Output	Report logged; message contained; affected account/device assessed; staff informed if needed
Human fallback / exception	If business-critical work cannot wait, use a known phone number or provider portal to verify; do not bypass checks because a message says it is urgent

1. **Stop.** Do not click, reply, open an attachment, share a code or make a payment.

2. **Preserve enough evidence.** Take a screenshot or forward the message as an attachment only through your approved reporting process. Do not forward a suspicious link to colleagues just to ask what they think.
3. **Report it.** Send the report to the nominated internal route. If an account has been accessed or a device may be infected, call the system owner as well.
4. **Verify independently.** Contact the claimed sender through an established channel if the request affects business activity.
5. **If someone clicked or entered credentials, act promptly.** Change the affected password from a known-clean device if possible, end active sessions where the service provides that option, review MFA/recovery settings and tell the email/service provider. Escalate to qualified IT support if malware or wider access is suspected.
6. **Record the outcome.** Note the service, time, action taken, user impact and whether other staff need a warning.
7. **Learn without blame.** Adjust the filter, process or short training reminder that would make the same request harder next time.

Build backups and recovery you can actually use

A backup is a copy that is separate enough from the original to help when the original is deleted, corrupted, stolen, encrypted by ransomware or unavailable. Syncing is useful, but it may copy a deletion or ransomware-encrypted file; check whether the service provides version history and how long it retains versions.

The NCSC recommends backing up the data the business needs to operate — potentially including websites, email, invoicing, documents, contacts and customer information — and testing that a backup contains what is needed and can be restored. It also recommends protecting online backups with two-step verification and keeping an external device disconnected when not in use.^[^ncsc-backups]

Design a proportionate backup plan

The familiar **3-2-1** approach is a helpful starting point: aim for at least three copies, on two types of storage, with one copy separate from the ordinary working environment. It is not a substitute for testing, ownership or understanding how a cloud provider's restore process works.

System or data	How often it changes	Backup / export method	Separate copy or version history?	Recovery owner	Test date	Notes
Website and database						
Cloud business files						
Email / critical mailbox data						
Accounting / invoicing						
CRM / customer records						
Product / job photos and project files						

Set it up step by step:

1. List the information you would need to resume work: customer contacts, open orders, current projects, accounting, website, email, approved templates and key supplier records.
2. For each item, find the provider's documented backup, export, retention and restoration options. Do not assume a provider takes a restorable copy for your particular account.
3. Select a combination of online backup/version history and a controlled offline or independent copy proportionate to the data and your ability to manage it.
4. Put MFA on the backup account. Give at least two authorised people a documented route to obtain access in an emergency, without sharing one personal password.
5. Record the recovery order. A firm may need access to email and cloud files before it can restore a brochure website, for example.
6. Restore a small, non-destructive sample to a safe location. Check that it opens, is the expected version and has usable permissions. Record what worked and what did not.
7. Put the next test in the calendar. Repeat after a material system change, not only after a disaster.

Do not present a backup as a guarantee against loss. A backup can be incomplete, too old, inaccessible, overwritten, compromised or too slow to restore. Testing reveals these issues while there is time to fix them.

Define recovery priorities in ordinary language

Ask two questions for each service:

- **How long can we work without it?** This is the recovery-time objective (RTO): the maximum tolerable downtime for that process.
- **How much recent information could we recreate?** This is the recovery-point objective (RPO): the maximum tolerable data gap.

You do not need formal IT terminology in daily conversation. A trades business might write: “We can work from printed job sheets for one day, but need current bookings restored by the next working morning.” A consultancy might write: “We can use phone and a contingency mailbox for a few hours, but need current client files and email access within one business day.” These are internal targets to guide choices, not promises to customers.

SOP: backup restore test

Field	Procedure
Owner	System owner, with a second person observing for critical data
Trigger / input	Monthly or quarterly calendar reminder; material system change; provider concern
Output	Test record showing whether selected data was restorable, readable and appropriately protected
Human fallback / exception	If a live system cannot safely be tested, obtain a provider-supported test method or qualified IT help; do not risk deleting production data to prove a point

1. Choose one meaningful file set, export or website/database component that is safe to restore as a test.
2. Confirm the backup date, source account and intended restore location.
3. Restore to a separate test folder, sandbox or non-production environment. Do not overwrite live data.
4. Open several files, check dates/versions, and confirm that required people can access them appropriately.

5. Record the time taken, gaps, errors, costs or provider steps that were unclear.
6. Correct the backup configuration, documentation or access control if the test exposed a weakness.
7. Record the next test date and tell the security coordinator of any unresolved issue.

Respond to an incident calmly and in order

A cyber incident can be a suspected stolen account, ransomware, website compromise, fraudulent payment, lost device, data exposure or service outage. You do not need to diagnose everything before taking sensible containment steps. You do need to avoid making it worse.

The NCSC's small-business response-and-recovery guide defines a cyber incident broadly as unauthorised access or attempted access to IT systems, including malicious or accidental events, and provides a UK reporting route for a live attack.^[^ncsc-response]

First hour: contain, preserve, assess

1. **Activate the incident lead.** Use a phone number or alternative route if email may be affected. State only known facts: what was noticed, when, which service/device and what action has already been taken.
2. **Protect people and stop risky activity.** Pause affected payment, login or data-sharing activity. Where a device may be infected, disconnect it from Wi-Fi/Ethernet if doing so is safe; do not keep experimenting with it. Do not destroy evidence or wipe it before taking advice.
3. **Secure accounts and provider access.** From a known-clean device, use the provider's documented account-recovery process, change compromised credentials, revoke sessions/tokens where available and check recovery email, forwarding and MFA settings.
4. **Contact relevant providers.** Notify the web host, cloud/email provider, payment provider/acquirer, bank, insurer or managed IT supplier through known contact details. Ask what immediate containment they recommend and record the case reference.
5. **Preserve facts.** Keep timestamps, screenshots, alerts, affected account names, transaction references and communications. Do not store unnecessary copies of exposed personal or payment data.
6. **Assess data and legal implications.** Determine whether personal data is involved, whether it may affect individuals and whether the ICO breach process needs to begin. Use qualified legal/data-protection help where needed.
7. **Communicate carefully.** Give staff one approved message and an escalation route. Tell customers or suppliers only when you have enough verified information and a reason to do so; do not make unsupported statements about cause, scope or resolution.
8. **Recover in a controlled order.** Rebuild or restore only after you understand the likely entry point and have a safe recovery plan. Test critical functions before returning the service to normal use.

Do not pay, negotiate with or make promises to an attacker without informed legal, insurer and specialist advice. Do not let an urgent ransom message determine the whole response.

Incident contact card

Keep this outside the systems most likely to be unavailable, for example in the controlled password manager and a secure printed/physical business-continuity file.

Contact / service	Purpose	Known number or portal	Account reference / note	Owner
Managed IT / security supplier	Device, network and recovery help			
Email / cloud provider	Account recovery / service status			
Website host / developer	Website containment and restoration			
Payment provider / acquirer	Payment or checkout issue			
Bank fraud contact	Suspicious transfer / account protection			
Cyber insurer / broker	Policy notification and approved support			
Data-protection adviser	UK GDPR breach assessment			

SOP: initial cyber-incident triage

Field	Procedure
Owner	Incident lead appointed by the business owner
Trigger / input	Suspected account compromise, malicious software, exposed data, fraudulent payment, website issue, lost device or provider alert

Field	Procedure
Output	Containment actions, incident log, provider contacts, risk assessment and recovery decision
Human fallback / exception	If the incident lead is unavailable, the named deputy follows this procedure; if there is a live significant attack, use NCSC/official reporting routes and specialist support rather than waiting for a routine meeting

1. Open the incident record and write the time, reporter, service/device, observable symptoms and immediate business impact.
2. Stop affected high-risk actions such as payments, data exports, new administrator invitations or sending from a suspected mailbox.
3. Contain the affected account or device using provider/IT instructions. Do not erase evidence or reset every unrelated system without a reason.
4. Contact the service owner and relevant supplier using known contacts. Record reference numbers and recommended actions.
5. Check whether personal data, payment data or a customer-facing service is involved. Start ICO/contractual/insurance assessment promptly where applicable.
6. Decide and document the current status: contained, investigating, recovering, monitoring or escalated.
7. Before returning to normal operation, verify access controls, basic function, outstanding risks and the message staff/customers should receive.
8. Within an agreed review period, hold a short learning review: cause if known, what worked, actions, owners and due dates.

Build a security toolkit that fits the business

Tools can support a process. They cannot decide which data you should collect, verify a supplier bank change or make a team report a mistake. Start with controls you can run consistently, then add capability when a real risk, client requirement or operational constraint justifies it.

The source material used named products, fixed price bands and broad outcome claims. Those change quickly and are not used here as recommendations. Instead, assess a prospective service against current documentation, contractual terms, support, data handling, account administration, compatibility and exit/recovery options.

A phased purchasing and improvement model

Stage	Aim	Typical capabilities to assess	Evidence of completion	What does not follow automatically
Foundation	Reduce obvious account, device and recovery weaknesses	Password manager; MFA; supported devices; automatic updates; basic backup; email filtering; access register; staff reporting route	Named owners; critical accounts protected; a restore test; written procedures	Protection from every attack or compliance certification
Growing team / higher data exposure	Manage access and improve visibility	Business password-management controls; managed devices or MDM; better email protection; monitored backups; security awareness refreshers; website monitoring; supplier review	Joiner/leaver evidence; update status; alert ownership; tested escalation route	That a provider will manage all obligations or that human checks are unnecessary
Higher impact / specialist support	Obtain depth beyond internal capacity	Independent assessment; incident-retainer option; managed detection/response; penetration testing where justified; specialist payment/privacy/security advice	Scope, approval, contract and remediation plan	A guarantee that systems cannot be breached or that a test covers every risk

A business may need a specialist earlier than the table suggests. Examples include health data, large volumes of personal data, regulated activity, critical client contracts, custom code, complex integrations, a recent incident or a payment environment beyond a hosted checkout. Involve someone competent for the risk; do not market a basic checklist as an alternative to specialist assessment.

Ask suppliers useful questions

Before adopting a new cloud, website, payment or security service, ask:

1. Who owns the business account, and how is access transferred if the original administrator leaves?
2. Which MFA, roles, logs and recovery routes are available on the actual plan we would buy?
3. What data does the service process, where is it held, who can access it and what happens at termination?
4. What backups, retention, exports and restoration options exist, and which are our responsibility?
5. How are security updates and incidents communicated? What support route and service limits apply?
6. Which third parties/integrations will receive access, and how can that access be revoked?
7. Can we test the product with limited data before a broad rollout?
8. What is the documented route to delete/export data and remove user access?

Save answers with the security map. Marketing descriptions and a sales call are not evidence that a capability is configured for your account.

Use free features wisely

Free or included features can be valuable: operating-system updates, device screen locks, authenticator apps, provider spam filters, browser updates, platform roles and basic uptime alerts. But “free” does not mean configured, compatible, sufficient for the risk or supported forever. Review whether a feature is enabled, who receives alerts and how you will recover if it fails.

Avoid installing network-analysis, vulnerability-scanning or security-testing tools just because they appear in an online list. Running an intrusive scan against a live site or supplier system without permission can disrupt services and create contractual issues. Ask the host, developer or qualified professional what is appropriate for your environment.

A realistic 30-day implementation plan

This is an **illustrative sequence**, not a promise that every business will be fully secure in one month. A regulated business, custom website, data migration or significant incident may need specialist work and more time. The value of 30 days is that it creates a visible starting point.

Week 1: understand and protect critical accounts

Day	Action	Owner	Completion evidence
1	Complete the security map for email, domain/DNS, website, payments, cloud files, accounting and devices.		Completed first-pass table
2	Name the system owner and administrator for each critical service; identify any shared logins.		Access-register draft
3	Set up or review the password manager; enable MFA on its owner account.		Owner and recovery record
4	Change passwords and enable MFA for email, payment, domain/DNS and hosting.		Critical-account checklist
5	Review website/payment/cloud administrator roles and connected apps.		Unneeded access removed
6–7	Write the offboarding trigger and payment-change verification route.		Approved two-step procedure

Week 2: stabilise devices, website and email

Day	Action	Owner	Completion evidence
8	List business devices, operating systems and update status. Flag unsupported devices.		Device list

Day	Action	Owner	Completion evidence
9	Turn on or check automatic updates for operating systems, browsers and approved apps.		Screenshot or admin record
10	Check screen locks, lost-device controls and separation of guest Wi-Fi where practical.		Device/network actions
11	Confirm website HTTPS, host/developer contacts, update/backup process and alert recipient.		Website record
12	Update supported website components using a backup/test/rollback process.		Change record and test result
13–14	Check email filtering and teach the team the report-and-verify route.		Meeting note and reporting address

Week 3: reduce data and prove recovery

Day	Action	Owner	Completion evidence
15	Complete the data inventory for customer, staff and commercial information.		Inventory draft
16	Review shared folders, public links, external guests and restricted data access.		Access changes logged
17	Define a basic retention/review point and update the privacy-notice action list.		Privacy task list

Day	Action	Owner	Completion evidence
18	Confirm payment flow, provider contacts and card-data rule.		Payment owner confirmation
19	Configure/confirm backups for priority systems and MFA on backup accounts.		Backup plan
20–21	Run a safe restore test and record gaps.		Restore-test log

Week 4: practise response and set the calendar

Day	Action	Owner	Completion evidence
22	Complete the incident contact card and store it in an accessible controlled place.		Contact card
23	Walk through a fictional phishing/payment-change scenario using the SOPs.		Exercise notes
24	Confirm the personal-data breach assessment/escalation route.		Owner and adviser details
25	Review monitoring/alert recipients for website, email, payments and backups.		Alert-owner list
26	Re-check outstanding critical access and update actions.		Revised access register
27–28	Hold a short staff refresher: verify, report, no blame, no shared passwords.		Attendance / notes

Day	Action	Owner	Completion evidence
29	Schedule monthly reviews, quarterly refreshers and annual specialist/coverage review.		Calendar invitations
30	Business owner reviews risks, signs off priorities and assigns incomplete work.		Action plan with dates

Make security a routine, not a once-only project

The routines below are deliberately short. If a review repeatedly takes too long, simplify the register or obtain help; do not abandon it.

Monthly review

Use the first working week of the month, or another predictable slot. The aim is to notice change: a new starter, an abandoned app, a failed backup, a website update or a suspicious login.

Review item	Check	Owner	Evidence / follow-up
Access	Joiners/leavers, role changes, shared folders, connected apps		
Accounts	MFA/recovery changes, unusual login alerts, privileged users		
Updates	Devices, browsers, website components, unsupported products		
Backups	Success alerts, capacity, one meaningful restore check on schedule		

Review item	Check	Owner	Evidence / follow-up
Website/payments	Errors, alert ownership, new integrations, provider notices		
Data	New data collection, shared links, privacy-notice changes		
Scams	Reported messages, payment changes, one relevant reminder		
Incidents	Open actions, insurer/provider issues, lessons learned		

Quarterly team refresher

Keep it practical and fair. Cover one current scam pattern, payment-change verification, the reporting route, a reminder that no manager should ask for a password/MFA code, and the manual fallback for a key process. Invite questions. Update the procedure if it does not match how work actually happens.

Annual owner review

Review insurance, business continuity, service contracts, critical suppliers, website and payment architecture, data inventory, retention, access model and security budget. Consider a qualified independent review where business impact, client expectations or technical complexity have increased. A small business does not need a large-enterprise programme; it does need to know where its competence ends.

SOP: staff or contractor access change

Field	Procedure
Owner	Hiring/line manager initiates; system owner approves and administrator completes
Trigger / input	New starter, role change, temporary contractor, leave date or urgent access removal
Output	Appropriate named access granted or removed; access register updated; business continuity protected

Field	Procedure
Human fallback / exception	If the administrator is unavailable, the pre-named deputy acts; do not give an emergency shared password just to start work faster

1. The manager states the person's role, exact services/folders needed, start/end date and approver.
2. The system owner chooses the lowest suitable role and creates a named account. Do not reuse another person's account.
3. The user enables MFA, receives the password-manager/security briefing and confirms the reporting route.
4. The administrator records the service, role, approver, start/end date and next review date.
5. For a role change or departure, remove old group memberships and sessions, then grant only the new required access.
6. On departure, disable accounts by the agreed time, transfer necessary business ownership, recover company devices and remove from shared folders, apps, website, payment, social and remote-access systems.
7. Review any credentials previously shared with the person. Change them or replace the shared method with a role/delegated access arrangement.
8. The manager confirms completion and records any exception that remains open.

SOP: monthly security review

Field	Procedure
Owner	Security coordinator; business owner reviews unresolved high-risk items
Trigger / input	Recurring monthly calendar reminder, material change or provider alert
Output	Completed review record, prioritised actions, evidence and next meeting date
Human fallback / exception	If the coordinator is absent, a deputy completes the basic checklist; issues beyond capability go to a qualified supplier rather than being guessed at

1. Open the previous month's action list and mark completed, delayed or newly risky items.

2. Check alerts and update status for email, passwords/MFA, devices, website, payment provider and backups.
3. Review joiners, leavers, contractors, shared links, administrator accounts and connected apps.
4. Select one realistic backup restore sample where due; record its result.
5. Review reported suspicious messages and any payment/bank-detail changes. Confirm that opt-outs and privacy matters have a responsible owner where relevant.
6. Add a concise action, owner and due date for each issue. Escalate high-impact account, payment, data or outage risks to the business owner promptly.
7. Share only the necessary outcome with staff: for example, a new scam warning or an updated process.
8. Schedule the next review and retain the record in the restricted security folder.

Standalone checklists

15-minute owner triage checklist

Use this today if you have not started:

- ☐ I know who can sign in as an administrator to email, domain/DNS, website, payment provider and cloud files.
- ☐ I can name the recovery phone/email route for the primary email account.
- ☐ MFA is switched on for the business email owner account and password-manager account.
- ☐ I have a known way to back up or export the data we need to keep working.
- ☐ I know whether the website platform and device operating systems are still supported.
- ☐ I have named an internal contact for suspicious messages and payment-change requests.
- ☐ I have found the known bank/payment/host/IT support contacts without relying on a new email.
- ☐ I have scheduled the first 30-minute security review.

Before a colleague starts or leaves

- ☐ Manager has written down services, folders, roles and end date.
- ☐ New user receives a named account, MFA and only needed access.
- ☐ No existing user password is sent to or shared with the new person.
- ☐ Access register has been updated.
- ☐ On leaving, accounts/sessions/groups and external app access have been removed on time.
- ☐ Company device, authentication factor and business records have been accounted for.

- ☐ Business ownership of files, shared mailboxes and service subscriptions has been transferred where necessary.
- ☐ Shared credentials or recovery routes have been reviewed and changed where necessary.

Before a website or checkout change

- ☐ Owner, developer/host contact and rollback route are recorded.
- ☐ Current backup/restore option is known and checked.
- ☐ Change is from a trusted, supported source and actually needed.
- ☐ A safe test/staging plan exists where the change could affect checkout or customer data.
- ☐ Admin access is named, limited and MFA-protected.
- ☐ Test list includes website display, contact forms, login, basket/checkout, payment confirmation and customer emails.
- ☐ Alert recipients and payment-provider/acquirer contacts are current.
- ☐ Change, results and remaining risk are recorded.

When a payment request or bank-detail change arrives

- ☐ I stopped before acting on the email/call/link.
- ☐ I checked the underlying order, contract or invoice.
- ☐ I used an existing known contact route, not the request's contact details.
- ☐ A second authorised person reviewed the change where the business procedure requires it.
- ☐ I kept a concise record of the verification without storing unnecessary secrets.
- ☐ I reported the attempt if it was suspicious or unauthorised.

Your security action workbook

This final page turns the guide into a decision. Complete it with the business owner or manager. The aim is a small number of owned actions, not a vague promise to “improve security”.

Top risks and first controls

Rank	Risk or weakness	Why it matters here	First control	Owner	Due date	Status / evidence
1						

Rank	Risk or weakness	Why it matters here	First control	Owner	Due date	Status / evidence
2						
3						
4						
5						

Security decision record

Decision	What we know	Assumptions or gaps	Decision / boundary	Owner	Review date
Password manager / access method					
Backup and restore approach					
Website / checkout ownership					
Payment-change verification					
Data / privacy escalation					
Incident contact route					

My next business action

The one change I will complete in the next seven days:

Owner: Due date:

What will show it is complete:

Who needs to know or approve it:

Official resources and source notes

The links below were checked on **9 October 2026**. Provider features, law, contracts and technical guidance can change. Follow the current primary source for your exact circumstances.

[^ncsc-small]: [NCSC — Small organisations guide to cyber security](#). Small-organisation security guidance.

[^ncsc-password-manager]: [NCSC — Password manager buyers guide](#). Password-manager deployment guidance.

[^ncsc-updates]: [NCSC — Keeping devices and software up to date](#). Update guidance.

[^ncsc-phishing]: [NCSC — Phishing attacks: defending your organisation](#). Phishing defence guidance.

[^ncsc-backups]: [NCSC — Backing up your data](#). Backup and restore guidance.

[^ncsc-response]: [NCSC — Small Business Guide: Response & Recovery](#). Incident response guidance.

[^ico-minimisation]: [ICO — Data minimisation](#). UK GDPR data-minimisation guidance.

[^ico-b2b]: [ICO — Business-to-business marketing](#). PECR and UK GDPR B2B guidance.

[^ico-breach]: [ICO — Personal data breaches: a guide](#). Breach assessment and reporting guidance.

[^pci-merchants]: [PCI Security Standards Council — Merchant resources](#). Merchant PCI DSS guidance.

[^pci-cvv]: [PCI Security Standards Council — FAQ 1574](#). Card verification-code storage rule.