



ASCENDEA

AI / BUSINESS GROWTH / CHECKLIST

30-Day Cyber Security Checklist for UK Small Businesses

A plain-English, four-week cyber security checklist for UK small-business owners and managers. It gives step-by-step actions for accounts, passwords and MFA, website and email protection, backups and restore testing, file access, staff reporting, monitoring, incident response and an ongoing review cadence.



Author: Rob Arnold

ascendea.ai

ASCENDEA EDITION · OCTOBER 2026 · v1.0

Free Ascendea resource

Your route through this resource

Before day 1: set up your working record	3
Week 1: protect the accounts that can unlock the business.....	5
Week 2: secure the website and business email.....	7
Week 3: make data recoverable and give people a clear process	9
Week 4: monitor, prepare a response and practise safely.....	11
Ongoing security maintenance	14
Your completion and action record	15
Official guidance used in this edition	16
Publication and use notice.....	17
References	17

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 practical four-week implementation plan for owners and managers

Author: Rob Arnold · Ascendea · <https://ascendea.ai/>

Edition v1.0 · October 2026

This checklist helps a small UK business put basic cyber security controls in place over four weeks. It is written for a business that uses email, cloud files, a website or online booking/shop system, and business accounts such as banking, accounting, payment, CRM or supplier portals.

Work through the tasks in order. Tick an item only when it has been completed and recorded. If you do not have permission to change an account, ask its owner or supplier to do it. Do not put passwords, verification codes or customer data in this document.

A completed checklist reduces some avoidable risks. It does **not** guarantee that a business will prevent every cyber incident, meet every contractual requirement, or comply with every legal obligation. The appropriate controls depend on the systems, data, suppliers and risks in your business. NCSC guidance for small organisations covers the same foundations: backups, protecting devices and accounts, and spotting scams. [1](#)

Before day 1: set up your working record

Choose one person to coordinate this checklist and one deputy. For a sole trader, the deputy might be an external IT support provider, accountant or trusted business contact who knows how to reach you in an emergency. The deputy should not receive your passwords unless there is a properly controlled recovery arrangement.

Create a simple record of the systems your business relies on. You can keep it in an access-controlled document. Record account names and support contacts, not passwords.

System or service	What it is used for	Account owner	Administrator or supplier contact	Important data held	Backup/recovery checked?
Business email	Customer and supplier communication				

System or service	What it is used for	Account owner	Administrator or supplier contact	Important data held	Backup/recovery checked?
Website, booking or online shop	Public enquiries or sales				
Domain name and website hosting	Keeps the site address and service active				
Cloud files	Documents, quotes, drawings or project files				
Finance and payments	Accounting, banking or payment service				
Customer system	CRM, booking, mailing list or order data				

Use these ground rules throughout

- ☐ **Keep ownership clear.** Record who owns the business email domain, domain name, website hosting, cloud storage and administrator accounts. A supplier can manage a service, but the business should know who can regain access if that supplier is unavailable.
- ☐ **Use a safe change process.** Before a significant change, note what will change, who approved it, how you will test it, and how you will undo it if needed.
- ☐ **Ask before testing.** Do not scan, attack or try to break into a website or supplier system unless the owner has given explicit written authorisation and you understand the limits. Use the safe exercise in Week 4 instead.
- ☐ **Keep personal and business access separate.** Do not create a critical business service under a departing employee's personal email address. If a sole trader uses a personal address for a business service, record the recovery route and protect that address as a critical account.

Week 1: protect the accounts that can unlock the business

Start with the accounts that would give someone the broadest access: business email, password manager, domain registrar, website administrator, cloud files, accounting, banking, payments and customer systems. NCSC advises using a password manager for unique passwords and protecting the manager itself with two-step verification. [2](#)

1. Set up a password manager and account register

A password manager is a tool that stores account credentials and can generate a different password for each account. It does not remove the need to protect its main account.

- ☐ **Choose the right setup for the business.** Check that the service works on the devices your people use and that it supports separate user accounts and a controlled way to share a business login where sharing is genuinely necessary. Do not choose a service solely because a supplier uses it.
- ☐ **Create the business owner account.** Use an account controlled by the business, not a personal address belonging to one employee. Add a named deputy or recovery contact only if the product supports that safely and you understand what access it gives them.
- ☐ **Create a strong, unique main password or passkey.** Keep the recovery instructions in a secure, agreed location. Do not send the main password or recovery codes by email, chat or ordinary text message.
- ☐ **Turn on multi-factor authentication (MFA) for the password manager.** MFA may be called two-factor authentication (2FA) or two-step verification (2SV). It means a stolen password alone should not be enough to sign in. [2](#)
- ☐ **Make the account register.** Add every critical account from the table above. Record its purpose, account owner, administrator, recovery email/phone, MFA status and last access review date. Do not record the passwords in the register.

Example: A two-person electrical contractor might list its shared inbox, cloud job folders, estimating tool, domain registrar, online banking, card-payment terminal portal and website host. The priority is not the number of accounts. It is knowing who can sign in, who can recover them and what needs protecting first.

2. Replace reused and weak passwords

- ☐ **Start with the highest-impact accounts.** Change passwords for business email, the password manager, banking and accounting, payment services, domain registrar, website administrator and cloud storage first.

- ☐ **Use the password manager to make a new password for each account.** Do not reuse a password from another work or personal account. The manager can generate and save it so nobody needs to memorise it.
- ☐ **Check shared logins.** Where several people currently use one password, see whether the supplier supports individual user accounts. If it does, create individual access and remove the shared login. If this cannot be done immediately, log the account owner, every authorised user and a date to replace it.
- ☐ **Remove passwords from unsafe places.** Look in notebooks left at desks, spreadsheets, unprotected documents, browser notes, old email threads and chat messages. Move useful credentials into the manager, then remove or securely destroy the old copy where appropriate.
- ☐ **Check for saved passwords on shared or public devices.** Sign out and remove saved passwords from devices the business does not control. NCSC cautions against saving passwords in a browser on a shared public device. [2](#)

3. Turn on MFA or passkeys for critical accounts

Start with the same high-impact accounts. NCSC recommends passkeys where a service offers them; where they are not available, use a strong unique password and 2SV. [2](#)

- ☐ **Open the account security settings.** Look for “Security”, “Sign-in”, “Login”, “MFA”, “2FA”, “2SV” or “Passkeys”. Each service uses different words.
- ☐ **Choose the strongest practical method the service supports.** A passkey, security key or authentication app may be available. If the only available second factor for a critical account is SMS, do not leave MFA off while waiting for a different method. Enable the available option, note the limitation and review it later.
- ☐ **Register the right devices.** Use a business-controlled device where possible. Avoid making a former employee's personal phone the only MFA device for a company account.
- ☐ **Store recovery codes safely.** If a service supplies recovery codes, place them in the protected business password manager or another agreed secure recovery location. Do not keep the only copy in the email account it is meant to recover.
- ☐ **Test a routine sign-in.** Sign out of one non-urgent account and confirm the authorised person can sign back in with MFA. Do not test your only business-banking access without checking the bank's support and recovery process first.
- ☐ **Record completion.** Update the account register with the method used, registered device or key holder, recovery location and date.

4. Review who has access and remove what is no longer needed

NCSC recommends limiting privileged access, reviewing it regularly and removing accounts that are no longer used or needed. [6](#)

- ☐ **List administrators.** For email, cloud files, website, domain, finance and customer systems, list who has administrator access. Ask each service owner to export a user list if available.
- ☐ **Remove former staff, contractors and old suppliers.** Disable their accounts, remove them from shared folders and revoke their access to the password manager. Do this before or on their last working day where possible.
- ☐ **Review connected apps and integrations.** In each important account, look for “Connected apps”, “Apps”, “Integrations”, “API keys” or “Third-party access”. Remove tools that are no longer used. If you are unsure what an integration does, ask the system owner before removing it.
- ☐ **Reduce administrator access.** Give people standard access for daily work and administrator access only where their role needs it. Avoid using a high-privilege administrator account for routine email and browsing.
- ☐ **Set a leaver checklist.** Write down the first five actions when someone leaves: disable their accounts, remove file and password-manager access, transfer any business files or mailbox ownership, collect business devices or keys, and update the access register.

Week 2: secure the website and business email

5. Check website ownership, HTTPS and updates

A website can be run by a web designer, host, ecommerce provider or internal employee. The business still needs to know the account owner and how to get help. A browser connection without a certificate warning is a basic operational check. It is not a complete assessment of the website's security.

- ☐ **Identify the website owner and supplier.** Record the domain registrar, hosting provider, website platform, web developer and emergency support route in the working record.
- ☐ **Open the public site in a browser.** Check that the address begins with `https://` and that the browser does not show a certificate or connection warning. If it does, stop and contact the host or web developer. Do not enter customer or administrator information until it is fixed.
- ☐ **Check domain renewal.** Confirm that the account contact details are current, the domain is registered to the business or agreed owner, and the renewal process is known. Do not rely on an old employee's email address for renewal notices.
- ☐ **List the moving parts.** Record the website platform or CMS, theme, plugins/extensions, forms, payment or booking services, and any analytics or marketing integrations. A web supplier can help make this list.

- ☐ **Make a full backup before changing website software.** Include the files, database and configuration information necessary to restore the site. Record where it is stored and how to request a restore.
- ☐ **Apply available updates carefully.** Update the platform, theme, plugins/extensions and integrations through their official administrator area or a trusted web supplier. For a simple site, make one meaningful update at a time, then check the homepage, contact form, booking or checkout route, and mobile view. For a complex or revenue-critical site, ask the supplier to test first in a suitable non-live environment.
- ☐ **Turn on safe automatic updates where appropriate.** Automatic updates can help, but they still need periodic checking. NCSC notes that updates can require a restart, sufficient storage or a manual step, and that backups should be in place before updating. [4](#)
- ☐ **Set an update owner.** Name the person or supplier who checks website and device updates each month. If a plugin is unsupported or its owner cannot explain why it is needed, plan its replacement or removal.

6. Strengthen email filtering and phishing reporting

Email is often the route into an account takeover, invoice fraud or malware incident. Good filtering helps, but a legitimate message can sometimes be filtered and a malicious one can still arrive. NCSC recommends using suitable cloud-email filtering or a proven filtering service, while making it easy for staff to report suspected phishing. [6](#)

- ☐ **Confirm the mail service and administrator.** Record the provider, the administrator account and how to contact support. Protect the administrator account with MFA.
- ☐ **Check that spam, phishing and malware filtering are switched on.** Ask the email administrator or provider which protections are included, whether they apply to all users by default, and whether there are any unreviewed quarantine or junk folders.
- ☐ **Agree how staff report suspicious messages.** Use the provider's reporting button if there is one, or give staff a named internal contact and a simple instruction: forward as an attachment or report it without clicking links or opening attachments. Make sure people can report a mistake promptly without blame.
- ☐ **Add a payment-change rule.** Never change bank details, approve a new payee or release an unusual payment solely because of an email. Confirm the request using a known telephone number or another previously agreed contact route. Do not use the number in the suspicious message.
- ☐ **Keep filtering rules under review.** If a legitimate supplier email is repeatedly blocked, adjust the rule with care. Do not automatically allow an entire outside domain unless the business understands the consequence.
- ☐ **Ask about email-domain protections.** If you send from your own domain, ask your email provider or web supplier to check the domain's anti-spoofing and privacy configuration. NCSC's

free “Check your cyber security” service can check important email-domain areas; it is separate from the retired Web Check and Mail Check services. [13](#)

Week 3: make data recoverable and give people a clear process

7. Implement automated, separated backups

A backup is a copy you can restore when a device fails, data is deleted, a supplier outage occurs or an incident locks files. Include the data the business needs to operate, not only documents on one laptop. NCSC's small-organisation guidance specifically includes websites, emails, invoicing, documents, contacts and customer information in its backup examples. [5](#)

- ☐ **Choose what must be recoverable.** Use the working record to list the website and database, email, quotations, job or project files, accounting records, customer information, configuration notes and other essential data. Check what your software supplier already backs up and what it does not.
- ☐ **Set a backup frequency.** Choose a frequency based on how much work you could afford to recreate. A retailer processing daily online orders may need more frequent backups than a small consultancy updating documents weekly. Record the choice and the reason.
- ☐ **Use the 3-2-1 rule as a planning check.** Keep at least three copies on two devices or storage types, with one copy offsite. NCSC describes this as a common method for resilient backups, but also says that 3-2-1 on its own does not make a copy offline. [12](#)
- ☐ **Keep at least one backup separate from the live environment.** A connected drive or accessible cloud backup may be affected by the same incident as the live data. Ask your provider whether it offers version history, recovery of deleted data, restricted backup access or another way to keep a recoverable copy apart.
- ☐ **Protect backup access.** Enable MFA for the backup account, limit who can modify backups and record the recovery route. Do not give everyday users unnecessary delete or overwrite rights.
- ☐ **Write down the practical arrangement.** For each critical system, record: what is backed up, where it is held, how often, who can restore it, the expected recovery method, and the latest successful test date.

8. Test a restore before an emergency

A green “backup complete” message is not the same as a successful recovery. NCSC says to check that a backup contains all important data and that you know how to restore it. [5](#)

- ☐ **Choose a low-risk restore test.** Start with a non-sensitive document or a test copy of a website file. Do not overwrite live customer data during a first test.

- ☐ **Follow the documented recovery steps.** Use the provider's official recovery process or ask the supplier to demonstrate it. Record every step that was unclear.
- ☐ **Check the restored item.** Confirm that it opens, is the expected version and can be used for its intended job. For a website, use a safe non-live location where possible.
- ☐ **Record the result.** Note the date, what was restored, where it came from, how long it took, who performed it, problems found and the next action. Do not treat one successful file restore as proof that every system can be restored.
- ☐ **Fix gaps.** If a system cannot be restored, escalate it to the supplier or IT specialist and set a due date. The appropriate response may be a better backup plan, clearer ownership, additional storage, or a documented manual fallback.

9. Restrict access to sensitive files and data

UK GDPR security is risk-based. The ICO says organisations should use appropriate technical and organisational measures, assess the risk of their processing, and ensure they can restore access to personal data after an incident. [10](#)

- ☐ **Separate ordinary and sensitive information.** Identify folders or systems containing customer data, staff information, financial records, contracts, identity documents, health information or other confidential material.
- ☐ **Check who can access each location.** In the file-sharing or CRM settings, review users, groups, sharing links and external guests. Remove access that is no longer needed. If a person only needs one project folder, do not give them the whole company drive.
- ☐ **Use role-based access where the service provides it.** For example, a bookkeeper may need accounting access but not the full customer document archive; an installer may need job details but not payroll records.
- ☐ **Set a sharing rule.** Staff should use the agreed, access-controlled business location rather than sending sensitive files as email attachments where a safer shared location is available. Do not create public links for confidential information.
- ☐ **Check devices too.** Apply screen locks, current operating-system updates and the business's agreed device policy. If staff use their own devices for business data, record what business data is permitted there and when access must be removed.
- ☐ **Escalate high-risk data.** If your business processes substantial volumes of sensitive personal data, regulated information, or data for a client under contract, ask a qualified data-protection or security adviser what additional controls are required.

10. Run a short, practical team session

The aim is not to turn staff into security specialists. It is to make sure they know the business's normal process, recognise an unusual request and report a concern quickly. NCSC warns that phishing training cannot teach everybody to spot every phishing attempt; technical measures and supportive reporting are also needed. [6](#)

- ☐ **Book a 30-minute session.** Include employees, regular contractors and anyone who uses business email, files, payments or customer records.
- ☐ **Explain the most important rules.** Cover unique passwords and MFA; how to report a suspicious message; the payment-change verification rule; the location of business files; and what to do if a device, account or data seems compromised.
- ☐ **Show two relevant examples.** Use anonymised examples such as a fake supplier invoice request, a delivery text, an unexpected document-sharing invitation or a customer message that asks for credentials. Do not use customer data in the examples.
- ☐ **Practise the reporting route.** Ask each person to find the phishing-report button or the named contact. Make sure nobody thinks they will be punished for reporting a click or mistake.
- ☐ **Write one page of staff instructions.** Keep it somewhere staff can find it. Include the internal incident contact, the payment-change rule and a reminder not to share passwords or MFA codes.
- ☐ **Record attendance and questions.** Use questions to improve the instructions. A repeated question often means the process needs simplifying.

Week 4: monitor, prepare a response and practise safely

11. Set up proportionate monitoring and alerts

Monitoring should tell a named person when something needs attention. It is not a promise that every problem will be detected.

- ☐ **Choose two contacts for alerts.** Use a business-controlled mailbox and a deputy, rather than a single employee's personal address. Make sure the contacts know what they are responsible for doing.
- ☐ **Turn on service notifications.** In the website host, ecommerce/booking provider and email administrator settings, enable available notifications for outages, security alerts, failed backups and administrator changes. Check which alerts are included before relying on them.
- ☐ **Use a simple uptime check for the public website if it matters to the business.** Configure it to check a page that customers use and send an alert to the two contacts. Test one notification and record how to contact the host if the site is unavailable.

- ☐ **Consider NCSC Early Warning.** UK organisations can register for the free NCSC service using their public IP addresses and domain names. It sends information about potential malicious activity, vulnerabilities and exposed services seen by its information feeds. It does not actively scan your network and must complement, not replace, other controls. [9](#)
- ☐ **Do not treat public web-mention alerts as intrusion detection.** A name alert can be useful for marketing or reputation awareness, but it does not establish whether a system has been compromised. The source task's Google Alerts suggestion has therefore not been retained as a security control.
- ☐ **Avoid obsolete instructions.** NCSC's Web Check and Mail Check were retired on 31 March 2026. Do not put an old Web Check or Mail Check setup guide into your plan. [13](#)

12. Create a one-page incident response plan

Print this plan or store it somewhere that remains available if business email is unavailable. NCSC says a basic incident response plan should include key contacts, escalation criteria, a basic process and consideration of legal or regulatory requirements. [7](#)

Fill in the missing information below before an incident happens.

Plan item	Your business decision
Incident coordinator and deputy	
IT/web/email support contact and out-of-hours method	
Banking/payment contact	
Insurer and policy/helpline details, if applicable	
Senior owner who can approve taking a service offline	
Data-protection lead or adviser	
Main systems and suppliers	
Where backups and recovery instructions are held	
Alternative communication method if business email is unavailable	
People authorised to speak to customers, suppliers or the media	

First actions when something seems wrong

- ☐ **Pause and record.** Write down what was noticed, when, who noticed it, which accounts, device, file or service may be involved, and any messages or error details. Do not circulate screenshots containing personal data more widely than necessary.
- ☐ **Tell the coordinator.** Use the contact route in the plan. If there is a suspected fraudulent payment, contact the bank or payment provider immediately using a trusted number.
- ☐ **Follow the provider's recovery or security process.** For a suspected account takeover, use a known clean device where possible, contact the provider and follow its account-recovery route. The authorised account owner should reset credentials, review MFA, sign out unwanted sessions and check privileged access as directed by the provider.
- ☐ **Contain only within your authority.** The plan should state who can disable an account, take a website offline or disconnect a device. Do not delete logs, wipe a device, destroy emails or make broad changes before the coordinator or appropriate specialist has considered the evidence and impact.
- ☐ **Escalate when the impact is unclear or serious.** Bring in the web host, managed IT provider, insurer, data-protection adviser, security specialist or other appropriate support. Do not guess about an attacker or promise an outcome to customers before facts are known.
- ☐ **Keep an incident log.** Record decisions, actions, times, people involved, supplier case numbers and information still missing. NCSC stresses the value of tracking findings and actions throughout an incident. [7](#)

If personal data may be involved

A cyber incident can also be a personal data breach, but not every breach is reportable to the ICO. The ICO's current small-organisation guidance says to start a log, contain the breach, assess risk to people, and report a breach that meets the reporting threshold without undue delay and within 72 hours of discovery. Where there is a high risk to people, they must be informed without undue delay. The ICO marks this guidance as under review following the Data (Use and Access) Act, so recheck it when an incident happens. [11](#)

- ☐ **Start the timer and the log.** Record the time the business became aware, not only the time the incident may have started.
- ☐ **Find the facts.** Identify what personal data may be affected, whose data it is, whether it has been accessed, lost, altered or disclosed, and what safeguards were in place.
- ☐ **Contain and assess.** Take proportionate action to stop further loss, then assess the likely risk of harm to the people affected. Use the ICO's current guidance and seek advice when needed.
- ☐ **Decide and document.** Record why the breach is or is not reportable. If it is reportable, submit an initial ICO report within the relevant timeframe and follow up with further information as required.

- ☐ **Communicate carefully.** If people need to be told, give clear, specific information about what happened, what they can do and where to get help. Do not use an incident to send unrelated marketing.

13. Practise a safe security exercise

The original source proposed simulated attacks and phishing. Do not ask an unqualified person to attack your website, collect colleagues' passwords or send surprise phishing messages. That can disrupt the business, create unnecessary risk and confuse a real incident.

Use one of these safer exercises instead:

- ☐ **Run a restore exercise.** Repeat the Week 3 restore test with a different important but non-live item. This tests an actual recovery capability.
- ☐ **Walk through an incident scenario.** Choose a situation, such as “the shared email inbox is sending strange messages” or “the website payment page is unavailable”. Read the one-page response plan and ask: who notices, who decides, who contacts the supplier, what records are needed, and how would customers be updated?
- ☐ **Use NCSC Exercise in a Box.** This is a free resource designed to help organisations practise their response in a safe environment; it includes exercises on ransomware, phishing, passwords and vulnerabilities, and does not require you to be an expert. [8](#)
- ☐ **Write the improvements down.** Assign an owner and due date to each gap. Examples include an outdated support number, a missing supplier contact, unclear authority to reset an account or a backup that cannot be found.
- ☐ **Use a specialist for technical testing.** If the business needs a penetration test or website security assessment, agree the scope, written permission, systems, timing and reporting route with a qualified provider before any testing begins.

Ongoing security maintenance

These reviews maintain the controls already put in place. The suggested times are planning prompts, not a certification standard. Keep a brief record of what you checked, what changed and who owns any follow-up.

Monthly: 30-minute owner check-in

- ☐ Check the account register for new administrators, leavers, old shared logins and unused integrations.
- ☐ Confirm critical updates were applied or have an owner and date.
- ☐ Check the latest backup status and carry out a small restore check on a rotating basis.
- ☐ Review website, email, host and Early Warning notifications. Close or escalate unresolved alerts.

- ☐ Check that the incident contact list still works and that the business has access to essential supplier accounts.
- ☐ Record one improvement or unresolved risk in the action table below.

Quarterly: team and supplier review

- ☐ Refresh the team session using a current scam pattern relevant to the business. Include regular contractors who use business systems.
- ☐ Revisit the payment-change rule and the phishing-report route.
- ☐ Review software and device support. Plan to replace systems that are no longer receiving security updates.
- ☐ Ask key suppliers whether security, backup, support or account-recovery arrangements have changed.
- ☐ Review the external access, shared folders and connected apps created since the last review.

Annually: management review

- ☐ Review the full working record, account register, backup/recovery evidence and incident plan.
- ☐ Reassess the business's important data, systems, suppliers and likely incident scenarios.
- ☐ Review contracts, customer requirements and any cyber-insurance policy with the appropriate adviser. Do not assume an insurance policy proves that the business has the required controls.
- ☐ Decide whether the business needs independent security, IT or data-protection advice because its systems, data, staff count or contractual obligations have changed.
- ☐ Approve a short improvement plan with named owners and dates.

Your completion and action record

Use this final table to turn the checklist into a working plan. A tick without evidence is easy to forget; a short record makes the next review faster.

Action or issue	Owner	Due date	Evidence or decision	Status / next review
Password manager and critical accounts protected				

Action or issue	Owner	Due date	Evidence or decision	Status / next review
MFA/passkey rollout complete or exception recorded				
Website ownership, HTTPS check and update owner confirmed				
Email filtering and payment-change process confirmed				
Backup arrangement and restore test recorded				
Sensitive-file access reviewed				
Staff reporting process practised				
Monitoring contacts and alerts tested				
Incident plan completed and exercise run				
Next monthly review booked				

Official guidance used in this edition

The technical and regulatory references below were checked on **9 October 2026**. Provider features and UK guidance can change, so recheck the relevant official material before making a material decision or responding to an incident.

Publication and use notice

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

This Ascendea edition is a **non-exclusive licensed adaptation** prepared as general business education. It does not claim exclusive ownership of the underlying licensed material. It is provided for your own learning and permitted end use. No resale, redistribution, private-label or editable-source rights are granted.

This is general cyber security and business education, not legal, compliance, insurance, IT-security or data-protection advice. It does not provide a security or compliance guarantee. Obtain appropriate professional advice for your systems and circumstances. This finished edition is available as a free Ascendea resource.

References

1. [NCSC Small organisations guide to cyber security](https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security)
<https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security>
2. [NCSC Managing your passwords](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers)
<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers>
3. [NCSC Multi-factor authentication for your corporate online services](https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services)
<https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services>
4. [NCSC Keeping devices and software up to date](https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date)
<https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date>
5. [NCSC Backing up your data](https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security/backing-up-your-data)
<https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security/backing-up-your-data>
6. [NCSC Phishing attacks: defending your organisation](https://www.ncsc.gov.uk/guidance/phishing)
<https://www.ncsc.gov.uk/guidance/phishing>
7. [NCSC Plan: Your cyber incident response processes](https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes)
<https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes>
8. [NCSC Exercise in a Box](https://www.ncsc.gov.uk/section/exercise-in-a-box/overview)
<https://www.ncsc.gov.uk/section/exercise-in-a-box/overview>
9. [NCSC Early Warning](https://www.ncsc.gov.uk/section/active-cyber-defence/early-warning)
<https://www.ncsc.gov.uk/section/active-cyber-defence/early-warning>
10. [ICO A guide to data security](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/)
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/>

11. [ICO 72 hours: how to respond to a personal data breach](https://ico.org.uk/for-organisations/advice-for-small-organisations/personal-data-breaches/72-hours-how-to-respond-to-a-personal-data-breach/)

<https://ico.org.uk/for-organisations/advice-for-small-organisations/personal-data-breaches/72-hours-how-to-respond-to-a-personal-data-breach/>

12. [NCSC Offline backups in an online world](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)

<https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world>

13. [NCSC to retire Web Check and Mail Check](https://www.ncsc.gov.uk/blog-post/retiring-mail-check-web-check)

<https://www.ncsc.gov.uk/blog-post/retiring-mail-check-web-check>