SMALL BUSINESS SECURITY

# Have I Missed Anything?

The 7-point cyber security check and 30-day action plan for sole traders and tiny businesses.

> Plain English. No jargon. No fear score. Written for businesses of 1–5 people with no IT department.

ArtificialGeek Version 1.0 · September 2026 artificialgeek.com

START HERE

# How to use this pack

**1**

### Answer the seven checks

Read each page and tick *Yes*, *No* or *Not sure*. *Not sure* counts as *No* until you have looked.

**2**

### Pick your top three

Every *No* is just an action, not a failure. Mark the three that would hurt most if they went wrong.

**3**

### Follow the 30-day plan

Page 12 puts the fixes in a sensible order: email and money first, then devices, backups, people, scams and your emergency plan.

### Your scorecard

| # | Check | Yes | No | Not sure | Fix first? |
|---|---|---|---|---|---|
| 1 | Business email | ☐ | ☐ | ☐ | ☐ |
| 2 | Money and critical accounts | ☐ | ☐ | ☐ | ☐ |
| 3 | Work devices | ☐ | ☐ | ☐ | ☐ |
| 4 | Files and backups | ☐ | ☐ | ☐ | ☐ |
| 5 | People and access | ☐ | ☐ | ☐ | ☐ |
| 6 | Scams and payments | ☐ | ☐ | ☐ | ☐ |
| 7 | First response | ☐ | ☐ | ☐ | ☐ |

There is no score out of 100 and no traffic-light verdict. A pattern of *No* answers tells you where to start; it does not tell you that you are “insecure”. If something is actively wrong right now, do not finish this checklist first: go straight to page 11.

### The one-minute sign-in ladder

When you turn on extra sign-in protection, choose the strongest option your account offers:

1. **Passkey or hardware security key** — strongest and hardest to trick.
2. **Authenticator app** — a rolling code on your phone.
3. **Text-message code** — weaker, but far better than nothing.
4. **Password only** — the one to fix first.

Never read a sign-in code out to anyone who contacts you, however official they sound.

CHECK 1 OF 7

# Business email

**Typical effort: 15–30 minutes** (our estimate; it depends on how many accounts and devices you have)

> **Why this matters.** Your business email is the master key. Password resets for almost everything else are sent to it, so whoever controls it can usually take over the rest.

| Check yourself | Yes | No | Not sure |
|---|---|---|---|
| My email sign-in uses 2-step verification (MFA) or a passkey. | ☐ | ☐ | ☐ |
| My email password is long and used nowhere else. | ☐ | ☐ | ☐ |
| My recovery email and phone number are current and I control them. | ☐ | ☐ | ☐ |
| I know which devices are signed in, and nothing looks unfamiliar. | ☐ | ☐ | ☐ |

## Do this now

1. Open your email provider's security or account settings (search "[your provider] account security").
2. Turn on 2-step verification. Choose a passkey or an authenticator app if offered; text codes are the fallback.
3. Set a long, unique password: three or four unrelated words, or a random one from a password manager. Do not reuse it anywhere.
4. Check the recovery email and phone number. Remove any you no longer control, then test that you can receive a code.
5. If backup or recovery codes are offered, save them offline (printed and kept somewhere safe), not inside the same mailbox.
6. Review "recent activity" or "signed-in devices" and sign out anything you do not recognise.
7. Look for mail rules: automatic forwarding or filters you did not create. Attackers use hidden forwarding to watch your inbox.

## Watch out for

- Password reset emails you did not request.
- "New sign-in" alerts you did not cause.
- Anyone asking you to read out a code that was just sent to you.

**You are done when**

2-step verification is on, the password is unique and saved, recovery details are tested, and unknown devices and mail rules are gone.

CHECK 2 OF 7

# Money and critical accounts

**Typical effort: 30–60 minutes** (our estimate; it depends on how many accounts and devices you have)

> **Why this matters.** A stolen bank, payment, domain, website-hosting or accounting login can stop a small business trading in an afternoon. These are the accounts to protect first.

| Check yourself | Yes | No | Not sure |
|---|---|---|---|
| I have a written list of the accounts that would hurt most if stolen or locked. | ☐ | ☐ | ☐ |
| Every account on that list has MFA or a passkey switched on. | ☐ | ☐ | ☐ |
| Each one has its own unique password, stored somewhere I trust. | ☐ | ☐ | ☐ |
| I know how account recovery works for each, and the recovery details are current. | ☐ | ☐ | ☐ |

## Do this now

1. Use the account register on page 13. List your top ten: bank, payment providers, domain registrar, website host, accounting or invoicing, cloud storage, social pages, key suppliers.
2. Turn on the strongest sign-in each one offers (see the ladder on page 2).
3. Check who is the registered owner of your domain name and hosting. It should be you, not a former web designer or employee.
4. Turn on alerts for new payees, new logins and changed details wherever the provider offers them.
5. Close or remove old logins, saved cards and integrations you no longer use.
6. Write down (offline) how you would recover each account if you lost your phone tonight.

## Watch out for

- Accounts opened in someone else's name (a web designer, an ex-employee).
- One shared login used by several people.
- "Verify your account" emails that link to look-alike web addresses.

**You are done when**

Your top accounts are protected and listed in the register, with the owner named on each.

CHECK 3 OF 7

# Work devices

**Typical effort: 30–45 minutes** (our estimate; it depends on how many accounts and devices you have)

> **Why this matters.** A phone or laptop that is out of date, unlocked or lost can hand over your email, files and saved logins. Modern devices already include good protection; it only works if it is switched on.

| Check yourself | Yes | No | Not sure |
|---|---|---|---|
| Every device is still supported and receiving security updates. | ☐ | ☐ | ☐ |
| Automatic updates are on for the system and apps. | ☐ | ☐ | ☐ |
| Every device (phones and tablets too) locks with a PIN, password or biometric. | ☐ | ☐ | ☐ |
| Device storage is encrypted and I can locate or erase a lost device. | ☐ | ☐ | ☐ |

## Do this now

1. List every device that touches business accounts, including personal phones and old laptops.
2. Install pending updates on each, then switch on automatic updates.
3. Retire or isolate anything that no longer gets security updates: keep it off business accounts.
4. Set a screen lock with a short timeout. Use a proper PIN or password, not 1234.
5. Turn on built-in device encryption where it is not already on, and enable “find my device” or the equivalent remote lock and erase.
6. For everyday work, use a standard user account rather than an administrator account where you can.
7. Install apps only from official app stores or the vendor’s own site.

## Watch out for

- Fake “your browser needs updating” pop-ups on websites.
- USB sticks of unknown origin.
- Laptops left in cars or on trains.

**You are done when**

All devices are supported, updating, locked, encrypted and findable.

CHECK 4 OF 7

# Files and backups

**Typical effort: 30–60 minutes** (our estimate; it depends on how many accounts and devices you have)

> **Why this matters.** Ransomware, a broken laptop, a deleted folder or a locked cloud account: a tested backup is how you carry on trading. A backup you have never restored is still an assumption.

| Check yourself | Yes | No | Not sure |
|---|---|---|---|
| I know which files and data the business cannot operate without. | ☐ | ☐ | ☐ |
| Backups run automatically. | ☐ | ☐ | ☐ |
| At least one backup copy is kept offline or in a separate account. | ☐ | ☐ | ☐ |
| I have restored a file from backup in the last six months to prove it works. | ☐ | ☐ | ☐ |

## Do this now

1. Write down the essential data (invoices, customer records, contracts, photos, accounts) and where each lives now.
2. Aim for three copies, on two different kinds of storage, with one kept off-site or offline.
3. Switch on automatic backup, using your system's built-in tool or a reputable service.
4. Keep one copy disconnected or in a separate account so ransomware on your computer cannot reach it.
5. Protect the backup account itself with MFA.
6. Restore test: pick three files, restore them to a new folder, open them, and write down the date.
7. Website: find out where your host keeps backups, download a full copy now and store it off the server.

## Watch out for

- Confusing "sync" with "backup": deletions and damage sync too.
- Backups that only sit on the same laptop.
- Never testing a restore.

### You are done when

Backups are automatic, one copy is offline or separate, and you have a dated restore test.

CHECK 5 OF 7

# People and access

**Typical effort: 20–40 minutes** (our estimate; it depends on how many accounts and devices you have)

> **Why this matters.** Former staff, freelancers and past web designers tend to keep access far longer than anyone remembers. Every unused login is an open door.

| Check yourself | Yes | No | Not sure |
|---|---|---|---|
| I know who can sign in to each critical account. | ☐ | ☐ | ☐ |
| Nobody shares a login for critical accounts. | ☐ | ☐ | ☐ |
| When someone leaves, their access is removed the same day. | ☐ | ☐ | ☐ |
| People have only the access their job needs. | ☐ | ☐ | ☐ |

## Do this now

1. For each critical account, list everyone who can sign in: staff, freelancers, your accountant, your web person.
2. Remove anyone who no longer needs access. If a shared password was known to them, change it.
3. Give people their own logins instead of sharing one.
4. Use the lowest permission that works (for example editor, not administrator).
5. Ask contractors to use MFA on any account that touches your business.
6. Write a short leaver checklist: accounts, devices, shared mailboxes, cloud storage, social pages, company phone numbers. Use it every time.
7. Make it safe to say “I think I clicked something”. Fast reporting matters more than blame.

## Watch out for

- An ex-developer who is still an administrator.
- Shared “info@” mailbox passwords passed around.
- Personal accounts used for business.

**You are done when**

Access is listed, leavers are removed, and no critical account relies on a shared login.

CHECK 6 OF 7

# Scams and payments

**Typical effort: 20 minutes** (our estimate; it depends on how many accounts and devices you have)

> **Why this matters.** Most successful attacks on small firms begin with a message that persuades someone to act: change bank details, pay an urgent invoice, approve a sign-in. The defence is a simple rule, not a clever tool.

| Check yourself | Yes | No | Not sure |
|---|---|---|---|
| I have a written rule for changed bank details and urgent payment requests. | ☐ | ☐ | ☐ |
| Everyone who handles money knows the rule. | ☐ | ☐ | ☐ |
| I deny and report sign-in approval prompts I did not start. | ☐ | ☐ | ☐ |
| I know how to report scam emails and texts. | ☐ | ☐ | ☐ |

## Do this now

1. Adopt the Payment Change Rule on page 10, print it and tell everyone who touches money.
2. Agree who can approve payments, and a second approver above an amount you choose.
3. Turn on bank and payment-provider alerts.
4. Learn the signs: urgency, secrecy, a change of payment method, a look-alike sender address, a link you did not expect.
5. Forward suspicious emails to report@phishing.gov.uk and suspicious texts to 7726 (both free).
6. Treat voice and video with care too: a call that sounds like someone you know can be faked. Verify through a number you already trust.

## Watch out for

- “Boss” messages asking for gift cards or an urgent transfer.
- Invoice redirection: “our bank details have changed”.
- Fake HMRC, courier or bank messages, and QR codes you did not expect.

**You are done when**

The rule is written, printed and known to everyone who handles money.

CHECK 7 OF 7

# First response

**Typical effort: 20–30 minutes** (our estimate; it depends on how many accounts and devices you have)

> **Why this matters.** The first hour after something goes wrong matters most, and it is the hour when people freeze. Deciding in advance who to call and what to do makes it far easier.

| Check yourself | Yes | No | Not sure |
|---|---|---|---|
| I have my bank's official fraud number saved in my phone. | ☐ | ☐ | ☐ |
| I know how to lock and reset my main accounts quickly. | ☐ | ☐ | ☐ |
| I know when a personal data breach must be reported (page 11). | ☐ | ☐ | ☐ |
| My emergency contacts are written down where I can reach them without my computer. | ☐ | ☐ | ☐ |

### Do this now

1. Complete the emergency sheet on page 11 and keep a copy offline.
2. Save your bank's fraud line from its official website, and remember that 159 connects you to most UK banks.
3. Store account recovery codes offline.
4. Decide who does what if you are unavailable.
5. Note your website host's support route and how to restore a backup.
6. If you have business or home insurance, check whether it includes a cyber or legal helpline, and save the number.
7. Bookmark the NCSC and Report Fraud pages listed on page 14.

### Watch out for

- Trying to work through a long checklist while an attacker still has access.
- Paying a ransom before getting advice.
- Waiting to tell your bank.

**You are done when**

Your emergency sheet is filled in and kept somewhere you can reach with no computer.

PRINT THIS. PIN IT UP.

# The Payment Change Rule

Nobody changes bank details, adds a new payee or acts on an urgent payment request because of an **email, text, call or message alone**.

1. **Stop.** Urgency and secrecy are the tell.
2. **Check another way.** Contact the person or company using details you already trust: an old invoice, your own records, or a website address you type in yourself. Never use the number or link in the message.
3. **Second pair of eyes.** Payments above £_____ need a second person to approve.
4. **Still unsure? Do not pay.** Report it and ask.

### Call-back script

"Hi, it is [name] from [business]. I have had a message asking me to change your bank details. I am checking with you directly before I change anything. Did you send it?"

Use a number from your own records. If they say no, do not reply to the original message: report it.

### If "your bank" rings you

Hang up. Wait a moment, then call **159** or the number on your card or the bank's official website. Real banks do not ask you to move money to a "safe account".

## Ten red flags

- Urgent, secret or "do not tell anyone"
- New or changed bank details
- Payment by gift cards, crypto or a different method than usual
- Sender address is one letter off
- You are asked for a sign-in code
- A link or attachment you did not expect
- Pressure from "the boss" who cannot take a call
- A voice or video that sounds right but arrived unexpectedly
- The message is perfectly written (AI makes tidy scams)
- Your gut says something is off. Pause anyway.

IF SOMETHING HAS GONE WRONG

# Your first hour

| | |
|---|---|
| **Someone got into an account** | Change the password from a device you trust. Sign out all other sessions. Turn on MFA. Check recovery details and mail forwarding rules. Tell contacts to ignore odd messages. Check bank and payment accounts. Use the provider's official recovery page. |
| **Money sent to a fraudster** | Call your bank straight away (159 or the official number) and ask them to try to recall or freeze the payment. Report it at reportfraud.police.uk or 0300 123 2040 (England, Wales and Northern Ireland; in Scotland call Police Scotland on 101). Keep emails, screenshots and payment references. |
| **Ransomware or locked files** | Disconnect the affected device from every network (unplug cable, turn off Wi-Fi). Do not connect backup drives to it. If it is a live attack on your business, call 0300 123 2040 (24/7). The NCSC and police do not encourage paying a ransom. Restore from clean backups. |
| **Lost or stolen device** | Lock or erase it remotely. Change passwords for accounts that were signed in. Ask your mobile provider to block the SIM. Report theft to the police. |
| **Customer data lost or exposed** | Write down what happened. If there is a risk to people, report it to the ICO within 72 hours of becoming aware (you can add details later). Tell affected people if the risk to them is high. Record every incident, even ones you do not report. |

## Your emergency sheet (fill in, keep a copy offline)

| | | | |
|---|---|---|---|
| **Bank fraud line** | | **Web host support** | |
| **Who does what if I am away** | | **Accountant / adviser** | |
| **Insurance helpline** | | **Recovery codes stored at** | |

**Useful, free and official:** reportfraud.police.uk · report@phishing.gov.uk (emails) · 7726 (texts) · ico.org.uk (72-hour breach guide) · ncsc.gov.uk (small organisations guide).

YOUR NEXT 30 DAYS

# 30-day action plan

> Small steps in the right order beat a big push you never finish. Tick each box when it is really done, not when you have started.

| Week | Focus | Done | Date |
|---|---|---|---|
| 1 | **Email and money.** Checks 1 and 2: MFA, unique passwords, recovery details, top-ten account register. | ☐ | |
| 2 | **Devices and backups.** Checks 3 and 4: updates, screen locks, encryption, automatic backup, one offline copy. | ☐ | |
| 3 | **People and payments.** Checks 5 and 6: remove old access, write the Payment Change Rule, brief everyone. | ☐ | |
| 4 | **Prove it.** Check 7: emergency sheet, restore test, and set your next recheck date. | ☐ | |

### My top three fixes

| | |
|---|---|
| 1 | |
| 2 | |
| 3 | |

### Recheck rhythm

Put these in your calendar now: a **15-minute monthly** look at alerts and access, and a **full re-run of this check every three months**. Also re-run it whenever someone joins or leaves, you change a key supplier, or you take on a new system.

WORKSHEET

# Critical account register

> **Never write passwords, recovery codes or PINs here.** This sheet records who and what, not secrets. Keep it somewhere safe.

| Account | Owner | Who has access | MFA / passkey | Recovery tested | Reviewed |
|---|---|---|---|---|---|
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |
| | | | ☐ | ☐ | |

Ideas for what to list: business email, bank, payment provider, domain registrar, website host, accounting or invoicing, cloud storage, social media pages, key suppliers, HMRC and Companies House logins.

REFERENCE

# Plain-English glossary

| | |
|---|---|
| **MFA / 2-step verification** | A second proof of who you are when you sign in, on top of your password. |
| **Passkey** | A sign-in that uses your device's lock instead of a password. It cannot be typed into a fake website. |
| **Phishing** | A message designed to trick you into giving something away or paying. It arrives by email, text, phone or social media. |
| **Ransomware** | Malicious software that locks your files and demands money to unlock them. |
| **Backup** | A separate copy you can restore from. It is not the same as syncing to the cloud. |
| **Password manager** | An app that creates and remembers unique passwords for you, so you only remember one strong one. |

## Where to get more help

- **NCSC small organisations guide:** ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security
- **Report fraud or a live cyber attack:** reportfraud.police.uk · 0300 123 2040
- **Report scam emails and texts:** report@phishing.gov.uk · 7726
- **Personal data breaches:** ico.org.uk → small organisations → 72 hours
- **Your bank:** 159, or the number on your card

### About this pack

ArtificialGeek is an independent site that explains technology in plain English. This pack is free, needs no email address and is not paywalled: essential safety help should never depend on buying anything. It is general guidance for small UK businesses, based on NCSC, Report Fraud and ICO material checked in September 2026. It is not legal, insurance or compliance advice, it is not a security certification, and following it cannot guarantee you will not be attacked. Guidance and products change, so check current official sources.