Small Business Cyber Self-Check

Regis Cyber · hello@regiscyber.com · regiscyber.com

A self-check for small businesses that do not have a full-time IT/security person. You can finish it in about 20 minutes.

> This is not a security audit. Nothing is tested, scanned, attacked, or verified by a third party. You answer 12 questions about how your business runs: accounts, backups, passwords, admin access, devices, email, vendors, and what happens in the first hour if something goes wrong.

Honest framing:

- You answer the questions.
- You score yourself.
- The score helps you prioritize. It is not a grade for an insurer, client, regulator, or lawyer.
- This is not a pentest, audit, certification, legal advice, privacy advice, insurance advice, or a guarantee of security.
- If you handle health, legal, regulated, or privileged client data, use this as a starting point and talk to a qualified advisor in your field too.

Best way to use it: do it once, alone, in one sitting. Then do it again two weeks later with whoever else helps run the business. The questions that make you pause are usually the ones worth fixing first.

Who this is for

- Solo founders and small teams
- Local service businesses
- Creators and agencies with client data
- Businesses using Google Workspace or Microsoft 365
- Owners staring at a vendor or cyber-insurance questionnaire and thinking, “I should probably know this”

The 12-question self-check

1. MFA is on for every important account

Check:

- email admin accounts

- banking/payment accounts
- domain registrar
- website hosting
- social accounts
- cloud storage
- password manager
- accounting/bookkeeping tools

Good sign: every owner/admin account uses app-based MFA or a security key.

Watch out: SMS-only MFA is better than nothing, but it is not ideal for high-value accounts.

2. Admin accounts are separate from daily-use accounts

Check:

- Do people use admin accounts for normal email and browsing?
- Are there old admin users from past staff/contractors?
- Does more than one trusted person know how to recover the business if the owner is unavailable?

Good sign: admin access is limited, named, and reviewed.

3. Passwords are in a real password manager

Check:

- no shared passwords in spreadsheets, text files, email threads, or chat apps
- each person has their own login where possible
- shared credentials, if unavoidable, live in a controlled vault

Good sign: every critical account has a unique password.

4. Backups exist and have been tested

Check:

- What gets backed up?
- Where does it back up to?
- Who gets alerts if backup fails?
- When was the last restore test?

Good sign: someone has restored a file from backup in the last 90 days.

5. Devices are patched

Check:

- Windows/macOS updates
- browser updates
- Microsoft Office/Adobe/Zoom updates
- router firmware
- NAS or server firmware

Good sign: updates are not months behind.

6. Endpoint protection is active

Check:

- Windows Defender or equivalent is running
- devices are not showing ignored malware alerts
- staff know who to contact if they see a warning

Good sign: antivirus/security status is visible and reviewed.

7. Email protections are not completely ignored

Check:

- SPF, DKIM, and DMARC exist for the domain
- staff know how to report phishing
- payment-change requests get verified out of band

Good sign: a fake invoice or payment-change email would not get approved by one person alone.

8. Critical vendors are known

List:

- email provider
- website host

- domain registrar
- payment processor
- accounting/bookkeeping platform
- cloud storage
- CRM/client database
- MSP/IT provider, if any

Good sign: you know who holds the keys to the business.

9. Offboarding is not improvised

Check:

- Can you remove a departing contractor from email, cloud storage, social media, password vault, website, and finance tools in one sitting?

Good sign: there is a short offboarding checklist.

10. Incident response has an owner

Check:

- Who decides what to do if email is compromised?
- Who calls the bank/payment processor?
- Who contacts clients if data may be involved?
- Where is the recovery checklist stored if email is down?

Good sign: the first hour after an incident is not pure guessing.

11. Devices and accounts are inventoried

Check:

- staff laptops/desktops
- shared devices
- phones with business access
- admin accounts
- software subscriptions

Good sign: you can answer “what do we have and who has access?” without digging for hours.

12. You have a 30-day cleanup list

Do not try to fix everything at once. Pick the biggest three:

- turn on MFA for admin accounts
- move passwords into a vault
- test one backup restore
- remove old users
- patch stale devices
- write a one-page incident plan

Quick score

- 10-12 green: good baseline; tighten documentation and evidence
- 7-9 green: workable, but there are likely gaps worth fixing this month
- 4-6 green: several basics are exposed
- 0-3 green: start with MFA, backups, and admin access immediately

This score is based on your own answers. It is not an audit, attestation, assurance engagement, certification, legal opinion, privacy opinion, insurance opinion, or something a third party should rely on as proof.

If this was useful

I would like to know one thing: which question made you stop and think?

That answer tells you what to fix first, and it tells me how to make this kit better.

If you downloaded this from the website, email hello@regiscyber.com with the number of that question. No pitch required.

If you want to keep going:

- The CAD $49 Starter Kit turns each question into a working tracker, with templates and a 30-day plan.
- The CAD $250 Working Hour is a one-hour screen share for owners who want help prioritizing.
- The CAD $895 Guided Checkup is for owners who want a written snapshot and a prioritized 30-day cleanup plan.

None of those are required to act on what you just learned.