FREE GUIDE

25-POINT CHECKLIST



The Small Business Cybersecurity Checklist

25 practical checks for Mid-Michigan businesses

CMIT Solutions · Tri-City & Flint, MI

Saginaw · Bay City · Midland
Flint · Frankenmuth

BEFORE YOU START

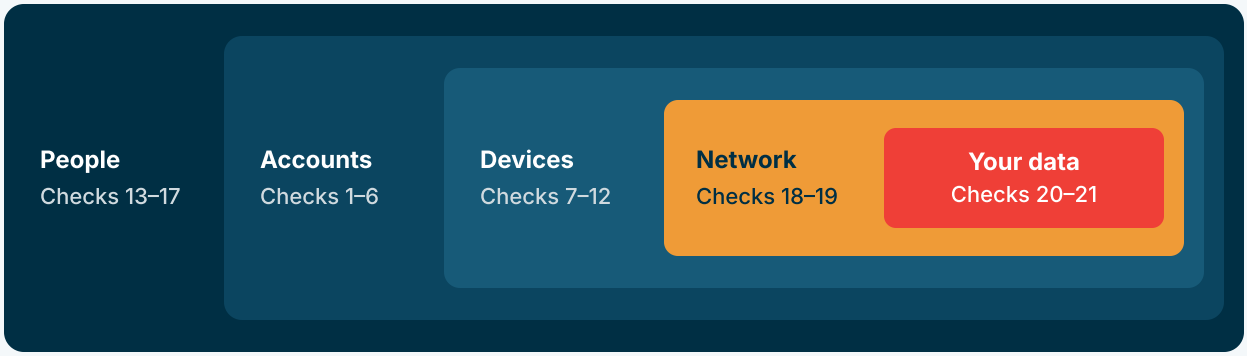
Who this checklist is for

If you run a business with a handful to a few hundred employees, you probably don't have a full-time security team. You may have one person who "handles the computers," an outside company you call when something breaks, or nobody at all. This checklist is for you.

It's written for owners, office managers and operations leads in Saginaw, Bay City, Midland, Flint, Frankenmuth and across Mid-Michigan who want a clear picture of where their business stands, without the jargon. None of the checks requires technical skills, and "I'm not sure" is a useful answer too.

How to use it

- [ ] **Sit down with whoever manages your IT** and go through the checks together.
- [ ] **Tick the box only when a check is fully in place.** If it's partly done, make a note of what's missing.
- [ ] **Start with the items tagged START HERE.** They close the most common gaps for the least effort.
- [ ] **Add up your score at the end** and use it to plan your next steps.



Layers of protection: each section of this checklist adds a layer between an attacker and your data. Plans and policies (checks 22–25) hold the layers together.

KEEP IN MIND

Security is a habit, not a product. No single tool makes a business secure. These checks work because they overlap. If one layer fails, another has a chance to catch the problem.

SECTION 1 · CHECKS 1–6

Accounts & passwords

Many break-ins start not with a sophisticated hack but with a stolen, guessed or reused password. Locking down accounts is high-value work.

- [ ] **01** **Turn on multi-factor authentication (MFA) for email.** START HERE
  Require a second step, such as an app prompt, a code or a security key, for every mailbox, including shared mailboxes and the owner's.

- [ ] **02** **Extend MFA to everything you can reach remotely.** START HERE
  Remote access tools, VPNs, cloud apps, payroll and online banking should all ask for a second factor.

- [ ] **03** **Use a business password manager.**
  Give staff a secure way to create and store long, unique passwords, so nobody reuses personal ones or relies on sticky notes.

- [ ] **04** **Separate admin accounts from everyday accounts.**
  Anyone who manages systems should read email and browse the web with a standard account, and sign in with a separate admin account only when they need it.

- [ ] **05** **Apply "least privilege."**
  Each person can reach the files, folders and systems their job requires, and no more. Review access whenever someone changes roles.

- [ ] **06** **Follow an offboarding checklist.**
  When someone leaves, disable their accounts, collect their devices and change any shared passwords they knew, on their last day.

> QUICK WIN
>
> Ask your IT contact to list every account that can sign in *without* MFA. That's your to-do list for checks 1 and 2.

SECTION 2 · CHECKS 7–12

Devices & software

Every laptop, server, phone and network device is a door into your business. Maintaining those doors closes many of the gaps attackers rely on.

- [ ] 07 **Keep an up-to-date inventory.**
  Know every device that connects to your network and every piece of software you use, and who is responsible for each.

- [ ] 08 **Patch operating systems automatically.** START HERE
  Turn on automatic updates and have someone confirm that they actually installed. A device that shows "update pending" for weeks is not patched.

- [ ] 09 **Patch everything else, too.**
  Browsers, PDF readers, accounting software, line-of-business applications and plug-ins need regular updates as well.

- [ ] 10 **Update firewalls, routers and Wi-Fi equipment.**
  Network gear has firmware that needs updating, and default admin passwords that must be changed before it goes into service.

- [ ] 11 **Run monitored endpoint protection on every computer.**
  Use modern protection that is managed centrally, so alerts reach someone who will act on them instead of a pop-up nobody reads.

- [ ] 12 **Encrypt laptops and retire unsupported systems.**
  Full-disk encryption protects data if a laptop is lost or stolen. Anything that no longer gets security updates needs a dated replacement plan.

> ASK THE QUESTION
>
> **"How would we know if a computer stopped getting updates?"** If the honest answer is "we wouldn't," that's the gap to close first.

SECTION 3 · CHECKS 13–17

Email, people & payments

Phishing emails and fake invoices target people, not machines. A trained, confident team is one of your strongest defenses.

- [ ] 13 **Train staff regularly.** Short, recurring awareness sessions and practice phishing exercises work better than a single annual lecture.
- [ ] 14 **Make reporting easy and blame-free.** Give everyone one simple way to report a suspicious message, and thank them when they do. Mistakes reported quickly are far easier to contain.
- [ ] 15 **Verify payment and banking changes by phone.** START HERE Confirm any request to change bank details or send a wire by calling a number you already know, never one from the email.
- [ ] 16 **Filter email and protect your domain.** Use business-grade filtering, and set up SPF, DKIM and DMARC records so it's harder for others to send mail pretending to be you.
- [ ] 17 **Set rules for personal devices.** If staff use their own phones for work email, require a screen lock, current updates and a way to remove company data if the phone is lost.

SECTION 4 · CHECKS 18–21

Network & data

- [ ] 18 **Separate guest and business Wi-Fi.** Visitors, smart TVs and other gadgets shouldn't share a network with your file server or point-of-sale systems.
- [ ] 19 **Know where your sensitive data lives.** List where customer records, financial data and employee files are stored, and who can reach them.
- [ ] 20 **Back up using the 3-2-1 approach.** START HERE Keep three copies of important data, on two types of storage, with one copy offsite, and ideally one copy that can't be altered or deleted.
- [ ] 21 **Test restores, not just backups.** START HERE A backup that has never been restored is a hope, not a plan. Schedule test restores and write down the results.

SECTION 5 · CHECKS 22–25

Plans & policies

Even well-protected businesses have incidents. What matters is how quickly you respond and recover.

- [ ] 22 **Write a simple incident response plan.** Cover who to call, what to disconnect, who can approve emergency spending, and how you'll communicate with staff and customers.
- [ ] 23 **Keep an offline contact sheet.** Print the numbers for your IT provider, bank, insurer and key vendors. If email is down, you can still reach them.
- [ ] 24 **Review your cyber insurance requirements.** Insurance applications and policies may ask about specific controls, such as MFA and backups. Make sure your answers match reality.
- [ ] 25 **Review vendor access, then repeat this checklist.** Check which outside vendors can reach your systems, and run through all 25 checks at least once a year.

IF SOMETHING LOOKS WRONG

Disconnect, don't delete. Unplug the affected computer from the network (leave it powered on if you can), call your IT contact and note what you saw. Don't reply, pay anything or try to fix it yourself.

Tally your score

Count one point for every box you ticked.

Your score	Where you stand	Suggested next step
21–25	Solid foundation	Keep testing restores, training staff and reviewing yearly.
13–20	Good start, with gaps	Prioritize any unticked checks in Accounts (1–6) and Network & data (18–21).
0–12	Time to act	Start with the six *Start here* checks (1, 2, 8, 15, 20 and 21) this month.

This score is a self-assessment, not a formal audit.

NEXT STEPS

How CMIT Solutions of Tri-City and Flint can help

Working through 25 checks while running a business is a lot. You don't have to do it alone.

CMIT Solutions of Tri-City and Flint is a locally owned managed IT provider based in Frankenmuth and led by owner Linton Pinnock. We help small and mid-sized businesses across Saginaw, Bay City, Midland, Flint, Frankenmuth and the surrounding Mid-Michigan area put practical security in place, and keep it there.

Walk through the checklist

We can go through these checks with you, explain what we find in plain English and help you set priorities.

Lock down accounts & devices

Help with rolling out MFA, managing updates and patches, endpoint protection and ongoing monitoring.

Back up and recover

Design backups around the 3-2-1 approach, keep an eye on them and run test restores so you know they work.

Prepare your people

Support with security awareness training, onboarding and offboarding steps, and a written incident response plan.

LOCAL TEAM, NATIONAL NETWORK

As part of CMIT Solutions, a network of 250+ locations across North America, we combine local, face-to-face service with the resources and shared experience of a larger organization.

Want a second opinion on your score?

Reach out through our contact page to start the conversation.
cmitsolutions.com/tri-city-flint-mi-1251/contact-us/

CONTACT US

CMIT SOLUTIONS OF TRI-CITY AND FLINT

Practical IT and security support for Mid-Michigan businesses

OFFICE

CMIT Solutions of Tri-City and Flint
1055 S Main Street, Suite A
Frankenmuth, MI 48734

SERVICE AREA

Saginaw, Bay City, Midland, Flint, Frankenmuth and surrounding Mid-Michigan communities

GET IN TOUCH

https://cmitsolutions.com/tri-city-flint-mi-1251/contact-us/

OWNER

Linton Pinnock
Locally owned and operated

CMIT Solutions · Tri-City & Flint, MI

This guide offers general information and best practices. It is not legal, insurance or compliance advice. © 2026 CMIT Solutions of Tri-City and Flint.