PHANTOM
Technology Solutions

PRACTICAL CHECKLIST

Cybersecurity Checklist

12 controls every small business needs. Use it today to find your gaps.

How to use this checklist

Go through each of the 12 controls below. For each one, mark whether you have it in place today. If you are unsure, mark it as a gap. At the end, tally your score using the guide on the last page. The goal is not to grade yourself, it is to find the specific places where your business is exposed so you can address them in priority order.

About these controls

These 12 controls are drawn from widely recognized security frameworks: the CIS Controls (published by the Center for Internet Security) and the NIST Cybersecurity Framework. They are not a complete compliance program, but they cover the controls that stop the majority of real-world attacks on small businesses. If you have all 12 in place and tested, you are ahead of most organizations your size.

1 Identity & Access

Most breaches start with stolen or guessed credentials. Controls 1 through 3 close the most common entry point attackers exploit.

Control	What good looks like
1. Multi-factor authentication (MFA) everywhere	MFA is enabled on every account your team uses: email, business applications, remote access, and admin portals, with no exceptions for convenience.
2. Strong unique passwords and a password manager	Every account has a unique password that is never reused, and your team stores credentials in a centrally managed password manager rather than spreadsheets or sticky notes.
3. Least-privilege access and prompt offboarding	Each person has access only to the systems and data their role requires, and when someone leaves, all accounts and access are removed the same day.

Start here if you are overwhelmed: If you can only do two things this month, enable MFA on email and business applications, and make sure your most recent backup has been tested. Those two actions eliminate the majority of your risk.

2 Devices & Data

Your devices and data are the targets. These controls ensure every endpoint is protected, software stays current, and your data can survive ransomware, hardware failure, or accidental deletion.

Control	What good looks like
4. Endpoint protection and EDR on every device	Every company computer and laptop runs modern endpoint detection and response (EDR) software, not just basic antivirus, and alerts are monitored by someone who acts on them.
5. Patch and update management	Operating system and software updates are applied on a defined schedule, typically within 14 days of release for critical patches, across all devices and servers.
6. Tested backups using the 3-2-1 rule	You keep three copies of critical data on two different media types with one stored offsite or in the cloud, and you have verified a full restore within the last 90 days.
7. Encryption: full-disk and in-transit	Full-disk encryption is enabled on every laptop and workstation (BitLocker on Windows), and all sensitive data is transmitted over encrypted connections only.

On backups: A backup you have never restored is not a backup, it is a guess. Schedule a quarterly restore test, recover actual files to a test location, and document that it worked. This is the step most businesses skip and regret.

3 Detection & Response

The question is not whether an attacker will attempt to get in, it is whether you will know when they do. Controls 8 through 10 make sure threats are filtered, contained, and seen.

Control	What good looks like
8. Email security and phishing filtering	Your email platform has active filtering for phishing links, malicious attachments, and impersonation attacks, and the filter is reviewed and updated regularly.
9. Network security: firewall, segmentation, and secure Wi-Fi	You have a business-grade firewall at your perimeter, guest Wi-Fi is isolated from internal systems, and any remote access uses a VPN or zero-trust solution.
10. Logging and monitoring with 24/7 detection	Security events from your endpoints, email, and network are logged and reviewed, ideally by a managed detection and response (MDR) service that can respond around the clock.

Detection is where most small businesses are weakest

You can have strong locks on the doors and still not notice when someone is already inside. If controls 8 through 10 feel out of reach to run in-house, this is the single most common reason small businesses move to a managed detection and response provider.

4 People & Process

Technology alone does not create security. Your team is both your greatest risk and your best defense, and the plan you write before an incident determines how badly one hurts. Controls 11 and 12 turn your people and your processes into an asset rather than a liability.

Control	What good looks like
11. Security awareness training and phishing simulation	Every employee completes security awareness training at least annually, and you run regular simulated phishing tests so staff practice recognizing attacks in a safe environment.
12. A written, tested incident response plan	You have a documented plan that tells your team exactly what to do in the first hour of a ransomware attack or breach: who declares an incident, who to call (IT, legal, insurance), and how to contain the damage. It is reviewed and practiced, not just filed away.

Building control 12

Your incident response plan does not need to be long. A one-page document that answers four questions is enough to start: Who declares an incident? Who do we call first (IT, legal, insurance)? How do we isolate affected systems? Where is our communication plan if email is down? Write it down, test it once a year, and store a printed copy offsite. We offer a ready-to-use Incident Response Plan template in this same resource library.

That is all 12 controls. Use the scoring guide below to interpret your results.

Scoring your results

Count how many controls you marked as fully in place. Use the scale below to interpret your score.

Score	Interpretation	Recommended next step
0 to 5 checked	Urgent gaps	Your business has significant exposure right now. Prioritize MFA, backups, and endpoint protection immediately and consider bringing in professional help.
6 to 9 checked	Solid foundation, work to do	You have meaningful controls in place, but the gaps that remain are real risks. Build a 90-day plan to close them in priority order.
10 to 12 checked	Strong posture	You are ahead of most small businesses. The work now is maintaining and testing what you have, keeping tools current, and revisiting this checklist annually.

Want us to run this assessment for you?

We offer a no-obligation security review for small businesses in Indiana and Michigan. We go through each of these 12 controls against your actual environment and give you a written summary of your gaps and a prioritized action plan. No sales pressure, no jargon.

Talk to PTS

hello@phantomts.com
phantomts.com
Indiana & Michigan, since 2010