



The 25-Point Security Checklist

The checks that separate a protected business from an easy target.

Most breaches don't come from clever hackers. They come from small gaps nobody got around to closing — a missing backup, an old account, a login without a second lock. **Every box you can't tick is a door worth closing.**

How to use it: go through honestly, check what's genuinely true today, then add up your score on page 2.

ACCESS & PASSWORDS

- ☐ Multi-factor authentication (MFA) is on for email, banking, and admin logins
- ☐ Everyone uses a password manager — no reused, shared, or sticky-note passwords
- ☐ Accounts are shut off the same day someone leaves the company
- ☐ Admin and owner-level access is limited to people who truly need it

EMAIL & PHISHING

- ☐ Spam and malware filtering is active on all business email
- ☐ Staff have had phishing / awareness training in the last 12 months
- ☐ Any change to payment or bank details is verified by a second channel
- ☐ Email is protected against spoofing (SPF, DKIM, and DMARC are set up)

NETWORK & REMOTE WORK

- ☐ A business firewall is in place and its default password was changed
- ☐ Guest Wi-Fi is separate from the network your business actually runs on
- ☐ Remote workers connect through a VPN, not open public Wi-Fi
- ☐ Unused accounts, software, and old hardware have been retired

DEVICES & ENDPOINTS

- ☐ Every computer and phone auto-installs security updates
- ☐ Business-grade antivirus / endpoint protection runs on all devices
- ☐ Laptops and phones are encrypted and lock themselves automatically
- ☐ Personal devices that touch company data follow the same rules

DATA & BACKUPS

- ☐ Critical data is backed up automatically, every single day
- ☐ A backup restore has actually been tested in the last 90 days
- ☐ At least one backup is offline or offsite, where ransomware can't reach it
- ☐ Staff can only open the files and systems their role requires

PEOPLE & PREPAREDNESS

- ☐ There is a written plan for what to do if you're breached
- ☐ One person or provider clearly owns security — it's not "everyone / no one"
- ☐ Your cyber-insurance requirements (MFA, backups, training) are genuinely met
- ☐ Vendors with access to your data have been vetted for their own security
- ☐ You would know within a day if something had gone wrong



Add Up Your Checks

Count every box you were able to tick, then find your range below. Be honest — the point isn't a good grade, it's knowing where your real gaps are.

21–25

STRONG

You're ahead of most businesses.

The fundamentals are in place. Your next win is documenting it — so audits, renewals, and insurance questionnaires stop being a scramble and become a five-minute export.

14–20

SOME GAPS

Solid foundation, soft spots.

You've done the obvious things. The unchecked boxes are exactly where most incidents start — and usually the cheapest to fix once someone names them.

7–13

EXPOSED

A single bad click could hurt.

Enough is missing that one convincing email or lost laptop could cause real damage. The good news: the highest-impact fixes are faster and cheaper than most owners expect.

0–6

AT RISK

The basics aren't in place yet.

You're not careless — you're busy, like most businesses we meet. The right move is to prioritize a short list of essentials rather than try to boil the ocean.

WANT TO KNOW EXACTLY WHERE YOU STAND? — IT'S FREE

- 1. Take the free Compliance Snapshot.** Fifteen quick questions, about 30 minutes. We send back a one-page scorecard within 24 hours — yours to keep, whether we ever work together.
- 2. We walk through it together** on a 30-minute call. What's solid, what's soft, and what it would actually cost to fix.
- 3. Start only when you're ready.** Founding-client bonus: your first 90 days of Security Awareness Training are on us — even if that's all you engage with for now.

WHY THIS BEATS “WE’LL GET TO IT”

Carriers now want proof of MFA, backups, and training before they'll renew — and they raise premiums when you can't show it. “Getting to it” is what this checklist looks like once someone else does it for you.

WHO YOU'D BE WORKING WITH

A two-person firm out of New Jersey, not a call center. You'll have our cell numbers. We'd rather be the people you think of when security comes up than the ones who scared you into a contract.

Book your free 30-minute call: hackerwatchdog.com • (201) 455-7746

**Scan to book instantly.**

Point your phone camera at the code to schedule your free 30-minute call.