INTERNATIONAL IT SOLUTIONS

The Miami Beach Small Business Cybersecurity Checklist

30 plain-English checks that show you — in about 15 minutes — exactly where your business is exposed, and what to fix first.

A free guide from International IT Solutions
Managed IT & Cybersecurity · Miami Beach, Florida

2026 Edition

International IT Solutions · 800 West Avenue, Miami Beach, FL 33139 · iitsolutions.online

How to use this checklist

Most small-business breaches don't start with a master hacker. They start with something ordinary: an old login that still works, a backup that quietly stopped running, an update nobody installed, an email that looked like it came from the boss. The good news is that the fixes are mostly ordinary too.

Go through each section and tick every box you can honestly say "yes, that's done" to. Don't guess — if you don't know, leave it unticked. The unticked boxes are your to-do list, roughly in the order a security professional would tackle them. The whole pass takes about 15 minutes.

When you're done, count your unticked boxes and check the score guide on the last page. And if you'd rather have a local team walk through it with you, the last page explains our free cybersecurity assessment — no obligation, no pressure.

1 Access, Passwords & MFA

☐ Multi-factor authentication (MFA) is turned on for email, banking, and every cloud app — starting with email, the account attackers want most.

☐ Passwords live in a password manager — not in spreadsheets, sticky notes, shared documents, or text messages.

☐ Every employee has their own login. There are no shared accounts like a single "frontdesk" sign-in used by five people.

☐ Factory-default passwords have been changed on the router, printers, cameras, and phone system.

☐ Admin accounts are reviewed monthly, and anyone who no longer needs admin rights has them removed.

2 Backups You Can Actually Restore

☐ Backups run automatically every day — and a real person checks that they succeeded.

☐ At least one backup copy lives offsite or in the cloud, separate from your office network.

☐ You have test-restored a file from backup in the last three months. A backup that has never been restored is a hope, not a backup.

☐ Backups cover your cloud apps too — Microsoft 365 and Google Workspace data needs its own backup, it is not automatic.

☐ Backups are protected (offline or immutable) so ransomware cannot encrypt them along with everything else.

3 Patching & Endpoints

☐ Operating-system and app updates install automatically. “Remind me later” is not a patching strategy.

☐ Every computer runs business-grade antivirus / endpoint protection that someone actually monitors.

☐ No computer is still running an operating system that no longer receives security updates.

☐ Laptops that leave the office have full-disk encryption on (BitLocker or FileVault), so a lost laptop is not a data breach.

☐ Someone owns the list of every computer, tablet, and phone that touches company data — and it is current.

4 Email Security

☐ SPF, DKIM, and DMARC records are published for your domain, so criminals cannot easily send email pretending to be you.

☐ Your team follows one hard rule: any request to change bank details or send a wire gets verified by a phone call to a known number — every time.

☐ Email filtering and anti-phishing protection goes beyond the basic built-in defaults.

☐ Automatic forwarding of company email to outside personal addresses is off, or monitored.

☐ Staff know how to flag a suspicious email in one step — and they actually do it instead of just deleting it.

5 People & Offboarding

☐ When an employee leaves, their access is disabled the same day — email, cloud apps, remote access, and door codes.

☐ HR and IT share a written offboarding checklist, so a departure never leaves a live login behind.

☐ Vendor and contractor accounts expire when the job ends, not “whenever we get to it.”

☐ Every new hire gets 15 minutes of security basics in week one: phishing, passwords, and exactly who to call.

☐ Everyone on staff can answer this question without hesitating: “If something looks wrong on my computer, who do I call?”

6 Network & Wi-Fi

☐ Guest Wi-Fi is completely separate from the network your business systems run on.

☐ The router / firewall runs current firmware, and its admin password is not the factory default.

☐ Remote access (VPN or remote desktop) requires MFA. There is no open remote-desktop port facing the internet.

☐ Point-of-sale and payment systems sit on their own network segment, away from office PCs and guest devices.

☐ Old devices and unused accounts are removed from the network — nothing unidentified is plugged in or connected.

Score yourself

0–5 unticked — Strong shape. Your basics are covered. Keep the routine going: monthly reviews, quarterly restore tests.

6–12 unticked — Normal, and fixable. Most healthy small businesses land here. Work the list top to bottom; the first two sections close the doors attackers use most.

13+ unticked — Let’s talk this week. Nothing on this list is exotic, but together these gaps are how small businesses end up locked out of their own systems. The free assessment below is built for exactly this.

Get a free cybersecurity assessment

We’ll go through this same checklist against your real setup — your email, your backups, your network, your people — and give you a short written report of what we found and what we’d fix first, in plain English. It costs nothing, it takes about 30 minutes, and the report is yours to keep whether you work with us or not.

Call (305) 771-3338

Email **sales@iitsolutionsweb.com** · Visit **iitsolutions.online**

International IT Solutions · 800 West Avenue, Miami Beach, FL 33139
Mon–Fri, 8am–6pm · 24/7 support for managed clients

© 2026 International IT Solutions. This checklist is general guidance for small businesses, not a guarantee of security — every environment is different, and threats change. Share it freely with other Miami Beach business owners; please credit the source.