THE BRAINSTORM BRIEF

The SMB Cybersecurity Checklist

The 15 fundamentals every small business should have locked down — in plain English.

Most small businesses aren't breached by movie-style hackers — they're caught by the basics left undone. You don't need a big budget or an IT team to be a hard target; you need these fundamentals done consistently, so work down the list, check what's already true, and fix the gaps.

ACCOUNTS & ACCESS

- [ ] **Turn on MFA (multi-factor authentication) everywhere it's offered**

  A stolen or guessed password is the most common way businesses get broken into, and MFA stops the vast majority of those account takeovers.

  Do this → Switch on MFA for email, banking, and every business app — prefer an authenticator app or a passkey, and use text-message codes only when nothing better is available.

- [ ] **Give every account its own password, backed by a password manager**

  Reusing one password means a single leak somewhere hands an attacker the keys to everything.

  Do this → Roll out a reputable password manager, generate a unique long password for each account, and let your team stop trying to memorize them.

- [ ] **Use least privilege and a separate admin account**

  When everyday accounts carry admin rights, one wrong click can give malware the run of your whole system.

  Do this → Give each person only the access their job needs, and keep a separate admin account that's used only to install or change things.

- [ ] **Cut off access the day someone leaves**

  Former staff, contractors, and forgotten vendor logins are easy-to-miss doors left standing open.

  Do this → Keep a simple list of every account and app, and disable a departing person's access the same day — including shared logins and remote access.

DEVICES & UPDATES

- [ ] **Turn on automatic updates and patch promptly**

  Most breaches exploit known flaws that an available update would have already closed.

  Do this → Enable automatic updates for operating systems, browsers, and apps, and don't let updates sit postponed for weeks.

- [ ] **Run business-grade endpoint protection on every device**

  Protection that's switched off, expired, or missing on a single laptop is all ransomware needs.

  Do this → Install reputable, business-grade endpoint protection on every computer — Macs included — and keep it turned on and updated.

☐ Turn on full-disk encryption

A lost or stolen laptop or phone only becomes a data breach when the drive isn't encrypted.

Do this → Switch on BitLocker (Windows) or FileVault (Mac) on every computer, and require a passcode on every phone so its storage stays encrypted.

DATA & BACKUP

☐ Back up with the 3-2-1 rule — and actually test a restore

A backup you've never restored is just a hope, and ransomware or a failed drive is the wrong time to find out.

Do this → Keep 3 copies on 2 kinds of media with 1 offsite, plus at least one copy ransomware can't reach (offline or immutable) — then restore a few files each quarter to prove it works.

☐ Lock down your cloud and SaaS accounts

Most of your data now lives in email and cloud apps, where extra admins and forgotten app connections quietly pile up risk.

Do this → Turn on MFA for every SaaS admin, keep the number of admins small, and regularly remove unused users and third-party app connections.

PEOPLE & PHISHING

☐ Train the team to spot phishing — and make reporting easy

A convincing email is still the most common first step in a business breach.

Do this → Run short, regular phishing training and give everyone a one-click way to report a suspicious message, with no blame for asking.

☐ Stop criminals from impersonating your email domain

Without email authentication, scammers can send messages that look like they came from your company to your customers and staff.

Do this → Have your IT provider set up SPF, DKIM, and DMARC records for your domain so mailbox providers can catch and block mail that fakes your address.

☐ Set one clear rule for safe AI use

Staff pasting customer data, contracts, or source code into free AI tools can leak it outside your control — the new shadow IT, often called shadow AI.

Do this → Write a one-page rule for what may and may not go into AI tools, and favor business AI plans that don't train on your data.

NETWORK & RESPONSE

☐ Secure your router and Wi-Fi, and keep the firmware updated

A router left on its factory password and default settings is an open front door to everything behind it.

Do this → Change the default admin password, turn on WPA2 or WPA3 encryption, update the firmware, and put guests and untrusted devices on a separate guest network.

☐ Protect data while it's moving

Sensitive information sent over an unencrypted or public connection can be read while it's in transit.

Do this → Make sure your websites and email use HTTPS/TLS, and use a trusted VPN whenever you work on public or untrusted Wi-Fi.

☐ Write down a simple incident-response plan

The middle of an attack is the worst possible time to work out who to call and what to do.

Do this → Keep one page you can reach even if systems are down: who to contact (your IT provider or MSP, insurer, bank, legal), how to isolate a device, and where your backups live.

How to use this: check off what's already true, then turn the blanks into your fix-it list — most gaps are quick, low-cost wins, and the highest-impact items are near the top. You're receiving this checklist because you subscribed to The Brainstorm Brief, Brainstorm's weekly plain-English AI and cybersecurity newsletter for small business; you can unsubscribe with the one-click link in any issue. Questions any time: admin@brainstorminnovative.com.

Brainstorm Innovative Technologies, LLC · 12409 Curley St., Suite 103, San Antonio, FL 33576