Your First 5 High-Impact Security Fixes

A free guide for small business owners

Sylvan Assurance, LLC

Version 1.0 · Updated 2026-09-14

Contents

Your First 5 High-Impact Security Fixes **1**
The actions that address the most common small or medium-sized business (SMB) attacks — in the right order . . . 1
Why these five? . . . 1
Fix #1: Enable MFA on email and finance (today — 30 minutes) . . . 2
Fix #2: Audit and remove old accounts (this week — 60–90 minutes) . . . 2
Fix #3: Move to a password manager (this week — 2–3 hours to set up) . . . 3
Fix #4: Create an offboarding checklist (this afternoon — 30 minutes to build) . 3
Fix #5: Verify your backups are actually recoverable (this week — 2 hours) . . 4
What comes next? . . . 4
Quick scorecard . . . 4

About This Guide **6**

Your First 5 High-Impact Security Fixes

The actions that address the most common small or medium-sized business (SMB) attacks — in the right order

Who this is for: Small business owners who know they need to do *something* about security but don't know where to start. This is not a thorough security programme. It is the highest-return starting point: the five controls that, together, sharply reduce exposure to the most common attack vectors targeting businesses like yours.

Time investment: Most of these can be completed in a single afternoon. A few require a few days of follow-through.

Why these five?

Cybersecurity is a deep field. There are hundreds of controls, frameworks, and best practices. For a small business with limited time and no security team, trying to do everything means doing nothing well.

These five fixes were chosen because: 1. They address the most common initial access vectors used against SMBs 2. Each is implementable without technical expertise 3. Each provides immediate, measurable risk reduction 4. Together, they significantly reduce exposure to the most common SMB-targeted attacks

---

Fix #1: Enable MFA on email and finance (today — 30 minutes)

What it is: Multi-Factor Authentication requires a second proof of identity (typically a code from an app on your phone) in addition to your password.

Why it's #1: Your email account is often the master key to your digital business. Anyone who controls your email can reset the password for many of your other accounts. MFA is widely recognised as one of the most effective steps against automated credential attacks. It is one of the highest-value actions in this guide.

Do this right now: 1. Open your email admin settings (Google Workspace Admin Console or Microsoft 365 Admin Center) 2. Find Security → Multi-Factor Authentication / 2-Step Verification 3. Enable it and set it to **required** (not optional) for all users 4. Have all employees install **Google Authenticator** or **Microsoft Authenticator** on their phones 5. Repeat for your accounting/finance tool (QuickBooks, Xero, etc.) and your bank's online portal

Rule: If a service offers MFA and you haven't enabled it, you have an unlocked door. Lock it today.

What not to use: SMS (text message) codes are better than nothing but should be a fallback, not the primary method. Use an authenticator app wherever possible.

Fix #2: Audit and remove old accounts (this week — 60–90 minutes)

What it is: Reviewing who currently has access to your business systems and removing anyone who should no longer have it.

Why it's #2: Dormant accounts belonging to former employees, contractors, or vendors are a persistent, silent risk. An attacker who gets hold of old credentials (through phishing, a breach database, or the former employee themselves) walks straight in through a door you forgot existed.

Do this now: 1. Open each service your business uses (email, accounting, CRM, cloud storage, website admin, payment tools) 2. Navigate to the user or member list 3. Remove or suspend anyone who no longer works with you: former employees, contractors, vendors whose engagement has ended 4. While you're there: check for any accounts you don't recognise 5. Note anyone who has admin-level access and doesn't strictly need it: downgrade them to the minimum required for their role

The rule of thumb: If they left, revoke access the same day. If you didn't, do it right now.

Going forward: Every time someone leaves (even a part-time contractor, even on good terms), completing the access removal is the first thing that happens, not an afterthought.

Fix #3: Move to a password manager (this week — 2–3 hours to set up)

What it is: A password manager generates and stores unique, strong passwords for every account so you never reuse passwords and never have to remember them.

Why it's #3: Password reuse is the fuel for credential-stuffing attacks. When one service is breached (and services get breached constantly), attackers take the leaked username/password combinations and try them everywhere else. If you use the same password across 10 services, one breach compromises all 10.

Do this: 1. Choose a password manager: **Bitwarden** (free, open source, excellent), **1Password** (paid, excellent UX), or **Dashlane** for business 2. Install it on every device and as a browser extension 3. Have every employee set one up (Bitwarden has a free individual plan and a low-cost Teams plan) 4. Over the next 2 weeks: whenever you log in to something, let the password manager generate a new unique password and save it

You do not need to change every password on day one. Change them as you log in. Within 30 days most of your important accounts will have unique, strong passwords.

The rule: One password, one place. If two accounts share a password, that's two accounts that can be compromised together.

Fix #4: Create an offboarding checklist (this afternoon — 30 minutes to build)

What it is: A written checklist that is completed every time someone leaves your business, covering every digital account that needs to be closed or transferred.

Why it's #4: This is Fix #2 put into practice. Fix #2 is the clean-up; Fix #4 is what keeps you from needing to clean up again. The most common reason former employees still have access is not malice. It's that nobody had a documented process for removing it.

Build this now: 1. Open a document (Google Doc, Word, or even a printed sheet) 2. List every service in your business that requires a login 3. For each service, list the specific steps to remove a departing employee's access 4. Add: "Change any passwords the departing person may have known" 5. Add: "Transfer any files they owned to a shared folder before deactivating" 6. Add: "Redirect their email to their manager for 90 days" 7. Designate one person as the owner of this checklist: they run it within 24 hours of any departure

The rule: The checklist does not run itself. Someone must own it. Without a designated owner, it will be forgotten every single time.

Fix #5: Verify your backups are actually recoverable (this week — 2 hours)

What it is: Confirming that your backups work, not just that they run, but that you can actually restore from them in a reasonable amount of time.

Why it's #5: Ransomware is among the most serious threats to SMB survival. The most reliable way to avoid paying a ransom is having a clean, working backup that isn't also encrypted. Most SMBs have backups they have never tested. Many discover on the worst day of their business life that the backup doesn't work, is in the same account as the encrypted data, or takes 3 weeks to restore.

Do this: 1. Identify your backup for your most critical system (typically email + financial data) 2. Confirm where it is stored and what credentials are used to access it 3. Confirm it uses **different credentials** from your main accounts (if your backup account uses the same login as your production account, a ransomware attack reaches both) 4. Pick one non-critical file, delete it, and restore it from backup: time how long it takes 5. If you don't know how to restore, find out now, not during an incident

The key point: If your backup is in the same cloud account as your data, protected by the same password, it is unlikely to survive a ransomware attack. You have a second copy that will be encrypted alongside the first.

What comes next?

These five fixes address the most common attack vectors. Once they're in place, the natural next step is a structured assessment of your full security posture across Identity & Access Management, Data Classification, Backup & Disaster Recovery (DR), and Patch Management.

The **Small Business Foundational Security Risk Assessment** covers all four domains with scored, practical guidance, building directly on the foundation you've established here.

Quick scorecard

Use this to track your progress:

Fix	Status	Completed By
Fix #1: MFA on email and finance	Not started / In progress / Complete	
Fix #2: Audit and remove old accounts	Not started / In progress / Complete	
Fix #3: Password manager deployed	Not started / In progress / Complete	
Fix #4: Offboarding checklist built	Not started / In progress / Complete	

Fix #5: Backup restore verified	Not started / In progress / Complete

Target: All five complete within 2 weeks of reading this guide.

About This Guide

This guide is produced by **Sylvan Assurance, LLC** and reflects more than twenty-six years of professional security experience in network security, information security, and incident response, translated into plain-language guidance for small business owners.

It provides **general guidance and recommended security practices**. It is **not** a professional security audit or legal advice. Every recommendation is **optional** - a widely accepted way to reduce a common risk - and following it reduces exposure to common attack patterns but **does not guarantee security or prevent any particular breach**. Responsibility for your business's security remains with you.

For full terms, see the Terms of Use provided with the SMB Security Assessment.

Copyright 2026 Sylvan Assurance, LLC. Not for resale.

Free to share unchanged with credit. Terms: sylvanassurance.com/licence/free/

Where to go from here

Scan for the full toolkit that builds on this guide.
sylvanassurance.com/go/toolkit-smb-security-assessment

Scan for the companion book - the full story, in plain English.
sylvanassurance.com/go/smb-security-playbook