SMB Human Error Firewall Checklist

A non-technical, no-excuses guide for businesses under 150 employees

Technology doesn't usually destroy small businesses. People do — when they're rushed, distracted, undertrained, or unsupervised. Use this checklist to spot the human mistakes that put your money, reputation, and customers at risk.

How to use: Mark ✓ **Yes** (we do this consistently) or ✗ **No/Not sure** (this is a weak point). Many "No" answers? It's time for a **Human Error Firewall Review**.

1. MONEY – Payments & Payroll

Payments

- ■ Any invoice over $_____ requires approval from two people
- ■ We never approve invoices from mobile email or screenshots alone
- ■ No banking or vendor changes without a live verification call to a known contact
- ■ Vendor change requests have a 24–72 hour cool-off period before money moves
- ■ "Urgent payment" requests are treated as an automatic red flag, not a rush order

Payroll

- ■ Payroll credentials are never shared
- ■ Payroll MFA is tied to a company-controlled device, not a personal phone
- ■ If payroll admin is out, someone else can run payroll immediately (no single point of failure)

2. MESSAGES – Email & Approvals

- ■ Every inbox clearly flags external senders
- ■ Staff are trained to escalate unknown or unusual requests, not "just handle it"
- ■ No one clicks links in shipping/tracking emails without going through a known login page
- ■ A/P does not react to PDFs with "invoice," "renewal," "contract," or "urgent" without verification
- ■ Any email using time pressure ("before end of day," "right now") is treated as a potential attack
- ■ One person with one click cannot empty a bank account or move major funds

3. ACCESS – Credentials & Login Security

- ■ Every employee has their own login to every system they use
- ■ No shared manager passwords for POS, CRM, or admin tools
- ■ No generic accounts like "employee1," "frontdesk," or "admin"
- ■ Password manager is enforced company-wide for critical systems
- ■ MFA is enforced on email, payroll, CRM, banking, and POS
- ■ If something goes wrong, we can see which user did what (no shared logins)

4. PEOPLE – Onboarding & Offboarding

New Hires

- ■ New hires get access only to the tools they need for their role
- ■ They receive phishing and approval-flow training before starting real work
- ■ Any temporary credentials expire automatically

Departing Staff

- ■ Accounts are terminated, not just passwords changed
- ■ Access to email, CRM, POS, payroll, and vendor portals is fully revoked
- ■ MFA tokens and app access are removed or reset
- ■ Company devices are returned or remotely wiped
- ■ No ex-employee still has working logins to any system

5. ESCALATION – Hitting the Brakes

- ■ We have named decision-makers who can freeze: Banking, Payroll, POS, Vendor accounts
- ■ Employees know who those people are and how to reach them quickly
- ■ We have a documented process: Stop → Notify → Freeze → Review
- ■ When something looks off, staff follow a clear escalation path (not ask around)

6. ACCOUNTABILITY – When Mistakes Happen

- ■ We have a reporting culture, not a blame culture. People can admit mistakes early
- ■ We have a "no secret fixes" rule — no one quietly patches serious issues alone
- ■ Front desk/admin staff don't troubleshoot invoices, logins, or payments on their own
- ■ Leaders encourage staff to speak up fast, so we find problems before money is gone

Need help tightening this up?

Schedule your Human Error Firewall Review with NerdsToGo

We'll map your weak points and fix the workflows that get companies burned.

■ **Find your local NerdsToGo: www.nerdstogo.com**