

SMB Security Checklist

Twelve things worth fixing this month. No signup, no email required – the whole thing is on this page.

This is the list we work through when assessing a small business environment. Most of it costs nothing but attention, and it is ordered roughly by how much risk it removes per hour spent.

You do not need us to do any of it. If you would rather have it checked properly against your actual environment, that is what a security assessment is for.

1. Multi-factor authentication is on everywhere it can be

Email, remote access, banking, payroll, domain registrar and any admin console. Credential theft is one of the fastest routes into a small business, and MFA blocks most of it outright.

How to check: List every service that holds money, mail or customer data, and confirm MFA is enforced rather than merely available.

2. A backup exists that ransomware cannot reach

A backup that is always connected is a backup that gets encrypted with everything else. You need at least one copy that is offline or otherwise out of reach of a compromised machine.

How to check: Identify one copy that an attacker on your network could not delete. If you cannot name it, you do not have one.

3. The backup has actually been restored, recently

An untested backup is a hope, not a control. Most failed recoveries are discovered during the emergency.

How to check: Restore one real file and one full system to a test location, and write down how long it took.

4. Every admin account is known and accounted for

Old admin accounts from former staff and former providers are a common way back in long after someone has left.

How to check: List every account with admin rights on email, servers, network gear and your POS. Remove the ones nobody can justify.

5. Patching happens on a schedule, not when someone remembers

Most breaches exploit something that had a fix available. The gap is process, not knowledge.

How to check: Set a fixed weekly window for operating systems, browsers and firmware, and a faster path for critical fixes.

6. Email is protected with SPF, DKIM and DMARC

Without these, anyone can send mail that appears to come from your domain, which is how invoice fraud against your customers usually starts.

How to check: Check that all three records exist for your domain and that DMARC is doing more than just monitoring.

7. Offboarding is a written checklist

Access that outlives employment is one of the most common findings in a small business review, and it is entirely avoidable.

How to check: Write down every system a departing person must be removed from, and who is responsible for doing it the same day.

8. Guest WiFi cannot reach business systems

Guests, contractors and personal phones should never share a network with payments, cameras or back-office machines.

How to check: From the guest network, try to reach your POS or a server. If it responds, the networks are not actually separated.

9. Payment systems are isolated from everything else

Card handling environments should be segmented so an infected office laptop cannot reach them.

How to check: Confirm your POS sits on its own network segment, and that only the devices that must talk to it can.

10. Staff use a password manager rather than reuse

Reused passwords turn one unrelated breach into a breach of your business. A manager makes unique passwords the easy option.

How to check: Deploy a password manager and check that shared logins live there rather than in a spreadsheet or on a note.

11. You can see what is happening on your endpoints

You cannot respond to what you cannot see. Basic visibility turns a silent compromise into an alert.

How to check: Confirm something is reporting endpoint health and alerts centrally, and that someone actually receives them.

12. There is an incident contact list, printed

During a real incident, email and chat may be the things that are down or untrusted. A list you can only open on a laptop is a list you cannot use.

How to check: Write down who to call in what order, including your IT contact, bank, insurer and key staff. Keep a paper copy.