



Cybersecurity Checklist for Small Business Owners

Use this cybersecurity checklist, adapted from the NIST Cybersecurity Framework 2.0 and insights from leading experts, to help you identify, prioritize, and implement the most critical actions to protect your business from cyber threats.

1. Govern (Decide Who's in Charge)

- ☐ **[Critical]** Assign one point person (you, a trusted employee, or an outsourced provider) to oversee cybersecurity.
 - ☐ **[Critical]** Determine what legal or regulatory rules apply to your business (e.g., FTC Safeguards Rule if you handle financial data).
 - ☐ Create simple, clear rules for passwords, device handling, and protecting customer data.
 - ☐ Review your cybersecurity measures at least once a year using this checklist. Recognize that small businesses are prime targets because criminals know defenses are often weaker.
-

2. Identify (Know What You Have)

- ☐ **[Critical]** Create a list all business devices and software tools in use.
 - ☐ **[Critical]** Prioritize your most important data: customer info, invoices, payment records.
 - ☐ Track who has access to business-critical systems (email, accounting, banking).
 - ☐ Review third-party services you rely on (payment processors, cloud tools) for any risks.
-

3. Protect (Make It Hard for Criminals)

- ☐ **[Critical]** Enable Multi-Factor Authentication (MFA) on all business-critical accounts and use authenticator apps instead of text codes where possible.
- ☐ **[Critical]** Use strong, unique passwords for each account and store them in a reputable password manager (and add these to the rules in step 1 above).
- ☐ **[Critical]** Enable a firewall on your business network/router.
- ☐ **[Critical]** Segregate your bank accounts: one for daily operations, another (at a different bank) for savings or reserves.
- ☐ **[Critical]** Keep personal and business devices separate — never mix banking and casual browsing.
- ☐ Limit admin access. Keep a separate login for sensitive tasks and store that securely offline.
- ☐ Require dual authorization for high-value or outgoing payments (ACH, wires, transfers).
- ☐ Keep all software and devices updated with the latest patches.

- ☐ Install and maintain basic antivirus/endpoint protection.
 - ☐ Use a VPN for any remote access to your business systems, especially over public Wi-Fi.
 - ☐ Train yourself (and your team) to spot phishing, spoofed invoices, scam calls, and malicious QR codes.
 - ☐ Have an alternate payment processing option available in case your main provider freezes funds.
-

4. Detect (Spot Issues Early)

- ☐ **[Critical]** Activate text or email alerts for suspicious account or login activity in banking, email, and key software.
 - ☐ **[Critical]** Check your financial accounts daily for suspicious transactions.
 - ☐ Review login logs in email and accounting software monthly.
-

5. Respond (Be Ready to Act)

- ☐ **[Critical]** Create a simple incident response plan: who to contact (IT support, bank, insurance), what to check, and how to notify customers if needed.
 - ☐ **[Critical]** Consider cyber insurance as part of your risk management plan, but do not rely on it as a replacement for strong security measures.
 - ☐ Require verbal verification or code words before making changes to vendor or customer payment details.
 - ☐ Maintain an emergency admin account for account recovery if compromised.
 - ☐ Keep important contact details (bank fraud department, IT help, insurance) stored offline.
-

6. Recover (Restore and Move Forward)

- ☐ **[Critical]** Back up important data regularly. Store at least one copy offline or in a separate cloud account.
 - ☐ Test your backups at least once a year to ensure you can restore them.
 - ☐ Store backup keys or passwords in a secure, physical location - not on your computer.
 - ☐ Draft a brief business continuity plan for operating during outages.
-

Related Resources

- [Episode 561: "Cyber Security for Small Business" with Gary Pica](#)
- [Episode 575: "Protect Your Business from Cyber Attacks" with Nick Mullen](#)
- [NIST Cybersecurity Framework](#)