FUSION1

FREE CHECKLIST · CYBERSECURITY BASICS

Small Business Cybersecurity Checklist

Most attacks on small businesses aren't sophisticated. They succeed because of a stolen password, an unpatched laptop, or a backup nobody tested. Work through this list with whoever manages your IT and check off only what you can confirm is in place today.

How to use: Check only what you can confirm is in place today, then total your checks at the end.

1 Accounts & access

___ / 5

- [ ] **MFA is required on email and every cloud app**
  Multi-factor authentication stops the large majority of password-based account takeovers.
- [ ] **Everyone uses unique passwords stored in a company password manager**
  No reused passwords, no spreadsheets, no sticky notes.
- [ ] **Daily-use accounts do not have admin rights**
  Admin tasks use separate, limited accounts so one click can't compromise everything.
- [ ] **Shared logins are eliminated or tightly controlled**
  Each person signs in as themselves so activity can be traced and access removed.
- [ ] **Former employees lose all access the day they leave**
  Including cloud apps, shared passwords, and remote access tools.

2 Computers & devices

___ / 4

- [ ] **Every computer runs managed endpoint protection (EDR)**
  Centrally monitored, not a free antivirus someone installed years ago.
- [ ] **Operating system and app updates install automatically and are verified**
  Critical security updates are applied within days, not months.
- [ ] **No computers run unsupported operating systems**
  Windows 10 reached end of support in October 2025; replace or cover with Extended Security Updates.
- [ ] **Devices are encrypted, lock automatically, and can be wiped remotely**
  BitLocker or FileVault on laptops, and remote wipe for phones that access company email.

3 Email & web

___ / 3

- [ ] **Advanced email filtering blocks phishing and malicious attachments**
  Beyond the default spam filter.
- [ ] **SPF, DKIM, and DMARC are configured for your domain**
  Makes it harder for criminals to send email that looks like it came from you.

- [ ] **External emails are tagged and DNS/web filtering blocks known malicious sites**
  Warning banners help staff spot impersonation; filtering protects users on and off the office network.

4 Network ___ / 3

- [ ] **A business-grade firewall is in place with current firmware**
  Default admin passwords have been changed.
- [ ] **Guest Wi-Fi is separated from the business network**
  Visitors and personal devices can't reach company systems.
- [ ] **Remote access uses a secure method with MFA**
  Never Remote Desktop (RDP) exposed directly to the internet.

5 Data, people & response ___ / 5

- [ ] **Backups follow the 3-2-1 rule with an offline or immutable copy**
  Ransomware can't encrypt or delete what it can't reach.
- [ ] **A restore has been tested in the last 90 days**
  A backup you haven't restored is a hope, not a plan.
- [ ] **Staff complete security awareness training at least annually**
  Ideally with periodic simulated phishing emails.
- [ ] **A written incident response plan lists who to call and what to do first**
  Stored somewhere you can reach if systems are down.
- [ ] **You've confirmed you meet your cyber insurance policy's security requirements**
  Many insurers require MFA, EDR, and tested backups to pay a claim.

Your score

Items checked: _____ of 20 = _____ %

90-100%
Strong
You have solid fundamentals. Review this checklist twice a year to keep it that way.

65-89%
Gaps to close
A good base with a few real exposures. Start with the unchecked items in the first two sections.

Below 65%
At risk
Several core protections are missing. Prioritize now, before an incident sets the agenda for you.

Want a second set of eyes?

FUSION 1 will review your results with you and show you which gaps to close first. No cost, no obligation.

Book a free IT review

Call or text 814-499-2119
Toll-free 888-279-9776