



Free Cybersecurity Checklist for Small & Midsize Businesses

Protect Your Business from Costly Cyber Threats

43% of all cyberattacks target small businesses. One weak password, one phishing email, or one missed update can cost you everything.

Use this quick checklist to see if your business is secure and where you can improve today.

Essential Security Foundations



1. Secure Your Access

- ☐ Use **strong, unique passwords** for every account
- ☐ Turn on **multi-factor authentication (MFA)** everywhere
- ☐ Remove old user accounts and unused devices
- ☐ Give employees **only the access they need** (least privilege)



2. Protect Your Data

- ☐ Back up your files **automatically every day**
- ☐ Keep one backup **offline or in the cloud**
- ☐ Test your backups — make sure they actually restore
- ☐ Encrypt sensitive data like client info and financials



3. Train Your Team

- ☐ Teach staff how to **spot phishing emails**
- ☐ Run quick security refreshers every few months
- ☐ Have a **simple "report suspicious email" process**
- ☐ Include cybersecurity training for all new hires



Warning: The 2024 KNP Logistics breach which shut down a 158-year-old company began with **one guessed password** and no MFA.



Best Practice:

Require MFA for all users it blocks **over 99.9% of automated attacks** (Microsoft, 2024).



Warning: In 2024, **70% of ransomware victims** couldn't fully restore their data because backups were also encrypted (Sophos State of Ransomware Report, 2024).



Best Practice:

Follow the **3-2-1 rule** keep **3 copies** of your data, on **2 types of storage**, with **1 offsite**.

Advanced Protection & Preparedness



4. Keep Systems Updated

- ☐ Turn on **automatic updates** for software and devices
- ☐ Regularly patch routers, firewalls, and remote tools
- ☐ Use reputable antivirus or endpoint protection



5. Secure Your Vendors

- ☐ Check that vendors follow basic cybersecurity standards
- ☐ Limit what outside partners can access
- ☐ Remove vendor access when contracts end



6. Be Ready for the Unexpected

- ☐ Create a simple **Incident Response Plan** who does what if hacked
- ☐ Store key contacts (IT, legal, FBI/CISA) in one place
- ☐ Review your **cyber insurance** and what it actually covers



 **Warning:** Unpatched systems caused **58% of SMB breaches** in 2023 (IBM Security Report).



Best Practice:

Schedule updates during off-hours and automate reboots it closes vulnerabilities **within hours instead of weeks**.



 **Warning:** Over **90% of cyber breaches** start with a phishing email (Verizon Data Breach Report, 2024). One click can cost your company thousands.



Best Practice:

Use short, quarterly phishing tests companies that train regularly see **up to 60% fewer successful attacks** (KnowBe4 2024 Benchmark).

Quick Self-Check

Question	Yes	No
Do you have MFA on all accounts?	☐	☐
Are backups tested and stored securely?	☐	☐
Have employees had phishing training in the past 6 months?	☐	☐
Do you review vendor access regularly?	☐	☐
Do you have a plan if ransomware hits tomorrow?	☐	☐

 If you answered "No" to even one question, don't wait!

Contact **Clearwell Digital** today at sales@clearwell.digital or call +1 (240) 801-6367 to schedule your **Free Cyber Risk Review**.

Need Help Securing Your Business?

Clearwell Digital helps Washington, D.C. area SMBs protect their data, systems, and reputation through practical cybersecurity solutions from audits to recovery planning.

 **Web:** <https://clearwell.digital>

 **Phone:** +1 (240) 801-6367

 **Email:** sales@clearwell.digital



 **Get a Free Cyber Risk**

Review: We'll evaluate your current setup and show you 3 quick ways to boost security this month.