FREE RESOURCE FROM DGVAS

IT & Security Checklist for Growing Businesses

Use this 25-point checklist to see where your business is protected and where it is exposed. It takes about 15 minutes. Tick each item you can answer **"yes"** to with confidence.

1. Tick
Mark every item that is true for your business today.

2. Count
Add up your ticks and check your score on page 2.

3. Fix
Start with the unticked items in the first two sections.

1. Passwords & Accounts

Stops most break-ins

- ☐ **Two-step sign-in (MFA)** is turned on for email, banking and every cloud account.
- ☐ Staff use a **password manager** and never share or reuse passwords.
- ☐ Each person has **their own account**; no shared logins for email or important systems.
- ☐ When someone leaves, their **access is removed the same day**.
- ☐ Only a few trusted people have **administrator** rights.

2. Email & Phishing

The #1 way attacks start

- ☐ Email has **spam and phishing filtering** turned on.
- ☐ Your domain has **SPF, DKIM and DMARC** set up, so scammers can't send email as you.
- ☐ Staff know to **call and confirm** any request to change bank details or pay an invoice.
- ☐ Your team has had **security awareness training** in the last 12 months.

3. Computers & Devices

Close the open doors

- ☐ All computers get **Windows/Mac and software updates** automatically.
- ☐ Every computer has **modern antivirus / endpoint protection**, managed and monitored.
- ☐ Laptops have **disk encryption** (BitLocker or FileVault) turned on.
- ☐ Phones that access business email have a **screen lock** and can be wiped if lost.
- ☐ You have a **list of all your devices** and who uses them.

4. Network & Wi-Fi

- [ ] Your office has a **business firewall**, kept up to date.
- [ ] The Wi-Fi uses a **strong password**, with a **separate guest network** for visitors.
- [ ] Staff working from home connect **securely** to business systems.

5. Backups & Recovery

Your safety net

- [ ] Important data is **backed up automatically every day**.
- [ ] At least one backup copy is kept **separate** (offsite or in the cloud) from your main systems.
- [ ] You have **tested restoring** files from backup in the last 6 months.
- [ ] Microsoft 365 or Google Workspace email and files are **backed up too**.

6. Plans, Website & Compliance

- [ ] You have a simple written plan for **what to do if you are hacked**, and who to call.
- [ ] Your website uses **HTTPS** and its software and plugins are kept **up to date**.
- [ ] Your website has been checked for **accessibility (WCAG 2.2 AA)**.
- [ ] If you handle health or card data, you know your **HIPAA or PCI DSS** requirements.

Your score (out of 25)

22-25 ticks	**Well protected.** Keep it up, and review this list every 6 months.
15-21 ticks	**Some gaps.** Fix the unticked items in sections 1, 2 and 5 first.
0-14 ticks	**At risk.** One phishing email or failed laptop could stop your business. Get help soon.

Want an expert to check for you?

Book a **free, no-obligation IT & security assessment** from DGVAS. We review your devices, email, accounts, network and website, then send you a short report of the main risks and what to fix first.

dgvas.com · info@dgvas.com · +1 (808) 938-5953

This checklist is general guidance, not a full security audit or legal advice. © 2026 DGVAS (Digital Value Added Services). Let's talk about business.