Other Guys IT OTHERGUYSIT

The Houston SMB IT Security Checklist

10 things every small business should check — today.

NOT YOUR AVERAGE IT GUYS

otherguys.tech · (972) 244-3009 · The Woodlands, TX

The Checklist

Go through each item honestly. Check the box if you're confident it's handled. No check = action item.

1

Password Policies HIGH RISK

WHY IT MATTERS

Weak or reused passwords are the #1 way attackers get into business systems. If your team is using "Company2024!" across multiple platforms, you're one breach away from a very bad week. Enforce minimum 14-character passwords, ban common patterns, and require a password manager company-wide — not optional, mandatory.

- [ ] We enforce a password policy with complexity requirements and a password manager.

2

Multi-Factor Authentication HIGH RISK

WHY IT MATTERS

MFA blocks over 99% of automated account compromise attacks. If someone gets your password, MFA is the lock on the second door. Enable it on every account that supports it — email, cloud apps, VPN, banking. Use authenticator apps or hardware keys; SMS codes are better than nothing but not great.

- [ ] MFA is enabled on all critical business accounts (email, cloud, banking, admin portals).

3

Endpoint Protection HIGH RISK

WHY IT MATTERS

Every laptop, desktop, and phone that touches your network is an entry point. Free antivirus isn't cutting it in 2026. You need EDR (Endpoint Detection & Response) that monitors behavior, not just known signatures. Make sure every device is enrolled, monitored, and has remote-wipe capability.

- [ ] All company devices have managed EDR/antivirus with centralized monitoring.

4

Backup Strategy HIGH RISK

WHY IT MATTERS

Ransomware doesn't care how big your company is. If you can't restore from backup, you're either paying or starting over. Follow the 3-2-1 rule: 3 copies of data, on 2 different media types, with 1 offsite. Test your restores quarterly — a backup you've never tested is a backup that doesn't exist.

- [ ] We have automated backups with offsite/cloud copies and have tested a restore in the last 90 days.

5

Firewall Configuration MEDIUM RISK

WHY IT MATTERS

A firewall that was set up three years ago and never touched since is barely better than no firewall. Rules drift, ports get opened for "temporary" reasons and never closed. Review your firewall rules quarterly, enable intrusion prevention, and make sure logging is turned on and being reviewed.

- [ ] Firewall rules have been reviewed in the last 90 days and firmware is current.

6

Email Security HIGH RISK

WHY IT MATTERS

90% of cyberattacks start with an email. Phishing has gotten scary good — AI-generated emails that look exactly like your vendor's invoices. Deploy SPF, DKIM, and DMARC records. Layer on advanced threat protection that scans links and attachments before they hit inboxes.

- [ ] SPF/DKIM/DMARC are configured and we use advanced email threat filtering.

7

Employee Security Training MEDIUM RISK

WHY IT MATTERS

Your team is either your strongest defense or your biggest vulnerability. Annual training doesn't work — people forget everything by February. Run monthly phishing simulations and short micro-trainings. When someone clicks a test phish, that's a coaching moment. Build the culture.

- [ ] Employees complete regular security awareness training with phishing simulations.

8

HIPAA / Compliance Basics MEDIUM RISK

WHY IT MATTERS

If you're in healthcare, legal, or finance in Houston, you're probably handling protected data. HIPAA fines start at $100 per violation and scale to $1.5M per category per year. Encrypt data at rest and in transit, control access with role-based permissions, and document everything.

- [ ] We've assessed our compliance requirements and have documented policies in place.

9

Patch Management MEDIUM RISK

WHY IT MATTERS

Unpatched software is an open invitation. The average time between a vulnerability being disclosed and an exploit appearing is now under 15 days. Automate OS and application patching on a weekly cycle, with critical patches deployed within 48 hours.

- [ ] OS and application patches are automated and deployed within defined SLAs.

10

Incident Response Plan MEDIUM RISK

WHY IT MATTERS

When (not if) something goes wrong, panic is not a plan. You need a documented, tested playbook: who gets called first, how do you contain the breach, who talks to customers. Run a tabletop exercise at least once a year. The companies that recover fast are the ones that practiced.

- [ ] We have a written incident response plan and have rehearsed it in the last 12 months.

How'd You Score?

Count your checkboxes. Be honest — this is for you, not us.

✅ 9–10 Checks: You're in Great Shape

You're ahead of 90% of Houston SMBs. Keep it up — security is maintenance, not a one-time project. Consider a penetration test to validate your defenses.

⚠️ 6–8 Checks: Solid Foundation, Real Gaps

You've got the basics but there are holes an attacker will find before you do. Prioritize unchecked items by risk level — reds first. A quick assessment can build a 90-day roadmap.

🚨 3–5 Checks: Significant Exposure

You're running with real risk. Businesses your size get hit every day in Houston. The good news: most of these can be addressed in 30-60 days with the right partner.

🔥 0–2 Checks: Call Someone Today

This is urgent. You're operating without a safety net. Start with MFA, backups, and endpoint protection. Get help.

Need Help Closing the Gaps?

Book a free IT security assessment. We'll go through this checklist with you, identify your biggest risks, and give you a clear action plan. No pitch, no pressure.

Book Your Free Assessment →

Other Guys IT — Not Your Average IT Guys
The Woodlands, TX · (972) 244-3009 · otherguys.tech