The Small Business Cybersecurity Survival Toolkit

7 Quick Wins to Avoid a 1-Star Rating with Hackers

Todd Gallentine

CTO | MG Computer

(630) 258-5005 | tgallentine@mgcomputer.com

Introduction:

Hackers rate businesses the way foodies rate restaurants:

- Easy to get in
- Quick payoff
- No one notices until it's too late

Unfortunately, many small businesses unknowingly score **5 stars** on this "Hacker Yelp." This toolkit gives you fast, affordable fixes to make sure your business gets **zero stars**—locked doors, no shortcuts, and no "specials" for cybercriminals.

1. The Hacker's Scorecard: What Hackers Look For

Hackers scan for the weakest links. Here's their checklist:

- **Weak or reused passwords**
- **Unpatched software**
- **Unsecured Wi-Fi**
- **Employees who click suspicious links**
- **No data backup plan**

If you check even one of these boxes, hackers see you as a 5-star target.

2. The $8 Coffee Rule: Cheap Security Costs More Later

If your cybersecurity costs less than your daily coffee, it's probably just as weak. Breaches cost small businesses **$200k+ on average.**

Smart Fixes that Don't Break the Bank:

- Use a password manager (strong, unique logins)
- Enable multi-factor authentication (MFA)
- Keep software and apps updated automatically

3. The Red Flags Test: Are You Already on a Hacker's Radar?

- Employees receive frequent phishing emails
- Customers report suspicious messages from your company
- Devices run slow or behave
- Unfamiliar logins on your accounts

If any of these sounds familiar, you might already be compromised.

4. Top 3 Small Business Weak Spots

1. **Email** – 90% of attacks start here. Use spam filters + MFA.
2. **Passwords** – Ditch sticky notes and weak logins. Password managers are a must.
3. **Wi-Fi** – Secure with WPA3, strong passwords, and no guest access to business networks.

5. Breach Prevention Quick Wins (This Week)

Here are **7 things you can do right now**:

1. Turn on MFA for email, banking, and file storage.
2. Update all devices and apps.
3. Use a password manager.
4. Back up your data to the cloud + offline.
5. Train employees with a 10-minute phishing demo.
6. Restrict admin access only to those who need it.
7. Review your Wi-Fi setup for security gaps.

6. The "Too Late" Stories

- **Phishing Gone Wrong**: A single click drained $80k from a small business account.
- **Ransomware Lockdown**: A company paid thousands in ransom after failing to back up files.
- **Customer Data Leak**: One unsecured Wi-Fi connection exposed hundreds of customer records.

Each of these could have been prevented with simple, low-cost steps.

7. The Cyber Resilience Checklist

Print this page and keep it on your desk:

Your Next Step

Need help securing your digital future?

Our team provides assessments, expert-led training, and customized cybersecurity strategies tailored to modern businesses.

- **Please feel free to contact us for a no-obligation consultation.**

Email: tgallentine@mgcomputer.com
Phone:(630) 967-2009
Website: www.mgcomputer.com
Social Media: @mgcomputer