Cybersecurity on a shoestring budget

Protecting your small business without breaking the bank

Your guide to affordable cybersecurity

We're happy to see you here, digging into another educational resource developed to help you protect your small business from cyberthreats without emptying your bank account.

Make cybersecurity work for your budget

Let's face it: You're already stretching every dollar to keep your business running. The last thing you need is another expensive line item. But here's the reality—protecting your business data isn't optional anymore.

Accenture's latest Cybercrime report revealed that almost **43% of cyberattacks are on small businesses—** yet only about 14% of those SMBs were prepared to face those attacks. Recovering from an attack can cost upwards of half a million dollars. For most small businesses, that could mean closing your doors forever.

The good news? You don't need a Fortune 500 budget to protect your business effectively. With the right approach, free tools, and smart strategies, you can build robust cybersecurity defenses that keep your business safe.

This guide will show you **practical, affordable ways to protect your business**, including:

- How to get professional-level protection on a startup budget.
- Free security tools that actually work.
- Where to invest your limited security dollars for maximum impact.
- Simple security measures you can implement today.
- Smart ways to train your team without expensive programs.

> **43% of cyberattacks are on small businesses...14% of those SMBs were prepared...**

Why small businesses are attractive targets

Small businesses have become prime targets for cybercriminals and understanding why can help you better protect yourself.

The numbers tell the story

According to recent studies, **43% of all data breaches impact small and medium-sized businesses**. Why? Because cybercriminals are opportunists who look for the easiest targets with the best return on their effort.

What makes small businesses vulnerable?

- **Limited resources:** Most small businesses don't have dedicated IT staff or security budgets, making them easier targets than larger organizations with robust defenses.
- **Valuable data:** Despite their size, small businesses still process credit cards, store customer information, and maintain financial records—all valuable to cybercriminals.
- **Supply chain access:** Small businesses often have access to larger companies' systems as vendors or partners, making them attractive stepping stones for attackers.
- **Less awareness:** Without dedicated security training, employees may not recognize threats like phishing emails or social engineering attempts.

The real cost of inadequate security

Before investing in security, consider what inadequate protection is already costing you:

- Lost productivity from dealing with spam and malware
- Time spent worrying about potential breaches
- Customer concerns about data security
- Manual processes that could be automated securely
- Potential liability from customer data exposure

Build your budget-friendly security plan

Creating a comprehensive security plan doesn't require expensive consultants or complex frameworks. Here's how to build one that works for your business and budget.

Start with a written security plan

Having a documented security plan is your first line of defense—and it's completely free to create.

Download free templates

The Federal Communications Commission offers a free Cyberplanner specifically designed for small businesses. The Small Business Administration also provides templates and guidance tailored to businesses like yours. These resources give you a professional framework without the professional price tag.

Essential components of your plan

Your security plan should cover:

- Password requirements for all accounts
- Rules for handling sensitive information
- Steps to take if you suspect a breach
- Guidelines for remote work
- Regular review and update schedule

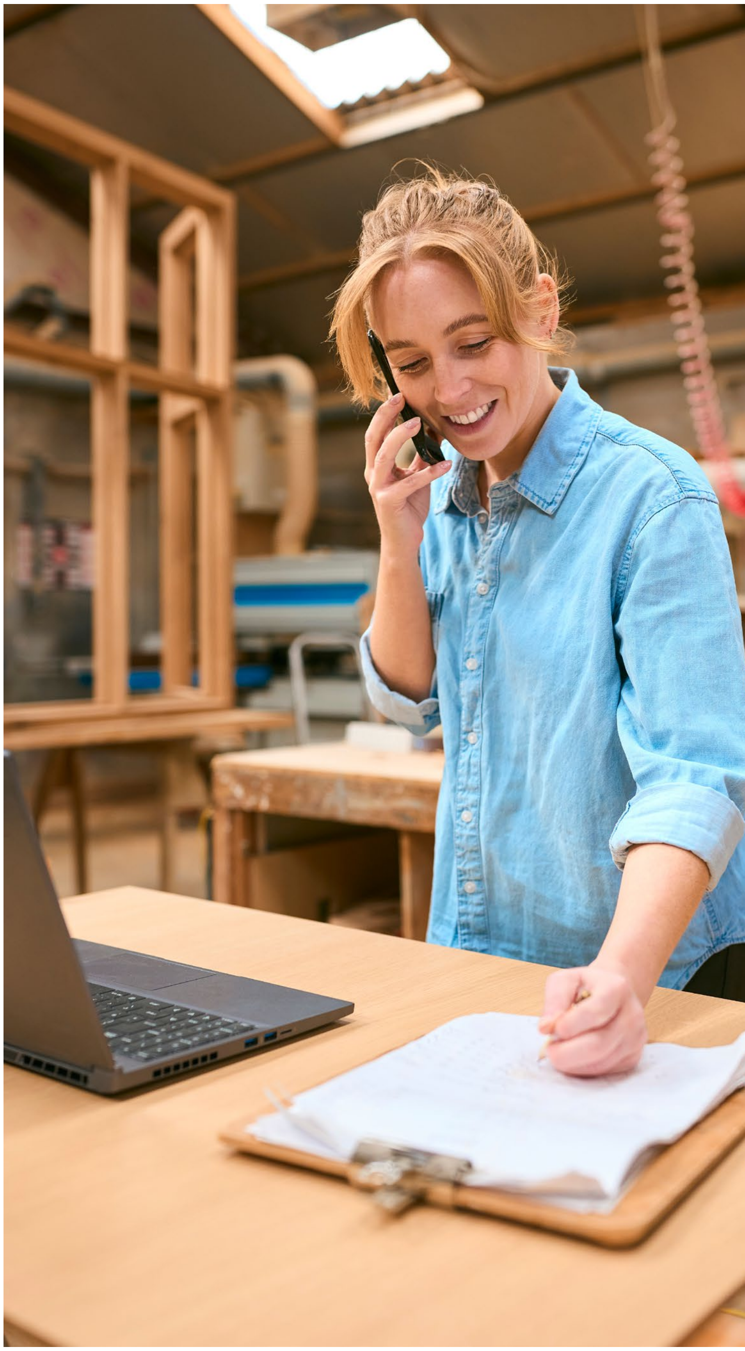
Implement strong password practices

Instead of complex passwords like "P@ssw0rd123", use memorable passphrases like "MyDogLoves2PlayFetchDaily!" These are easier to remember, harder to crack (and free to implement.)

Enable multifactor authentication (MFA)

Adding MFA to your accounts blocks 99% of automated attacks. Free options include Google Authenticator, Microsoft Authenticator, and Authy.

Even using SMS codes (text messages) is better than passwords alone, though app-based MFA is more secure.



Train your team without breaking the bank

Your employees can be your strongest defense or your weakest link. Here's how to build security awareness without expensive training programs.

Free government resources

Cybersecurity & Infrastructure Security Agency
Free online courses, downloadable training materials, and industry-specific guidance.

Small Business Administration
Cybersecurity basics for small businesses, best practices guides, and incident response planning.

Federal Trade Commission
Practical security tips, data security planning tools, and breach response guidance.

Create an in-house training program

Weekly security tips
Start each team meeting with a 5-minute security topic. Practice identifying phishing emails, provide strong password examples, teach employees how to maintain a secure device, or website browsing best practices.

Real-world examples
Share news stories about breaches at similar businesses. Real examples make abstract threats concrete and memorable.

Practice scenarios
Run simple drills like spotting fake emails, reporting suspicious activity, and following incident response steps.

Recognition over rewards
Celebrate security-conscious behavior with recognition rather than expensive rewards. A "Security Star of the Month" costs nothing but builds a culture of awareness.

Next up...

Free and low-cost security tools →

Essential free and low-cost security tools

You don't need expensive software to protect your business. Here are professional-grade tools that fit any budget.

Antivirus and anti-malware

- Microsoft Defender (built into Windows)
- Avast Free Antivirus
- AVG AntiVirus Free
- Malwarebytes Free (for on-demand scans)

Firewalls

- Windows Firewall (built-in)
- macOS Firewall (built-in)
- ZoneAlarm Free Firewall

Password managers

- Bitwarden (free for personal use)
- KeePass (open source)
- Browser-based managers (Chrome, Firefox, Edge)

Cloud storage

- Google Drive: 15GB free
- Microsoft OneDrive: 5GB free
- Dropbox: 2GB free

Budget backup tips

✓ Use multiple free accounts for more space

✓ Invest in a $50 external hard drive

✓ Rotate drives between office and home

✓ Partner with another business for offsite storage

The 3-2-1 backup rule

Keep 3 copies of important data, on 2 different media types, with 1 copy offsite. You can achieve this with free cloud storage and an inexpensive external drive.

3 quick wins you can implement today

Don't wait for the perfect plan. Start with these three steps today...

① **Enable MFA on your email**

Approx. time to complete: 5 minutes

This single step blocks most account takeovers.

② **Turn on automatic updates**

Approx. time to complete: 10 minutes

Patches fix known vulnerabilities.

③ **Back up critical files**

Approx. time to complete: 30 minutes

Use free cloud storage to protect essential data.

Where to spend when you must

If you have budget for security, prioritize these investments:

1. **Email security ($20-50/month):** Filters out most threats before they reach you.
2. **Managed antivirus ($30-50/month):** Centralized protection and monitoring.
3. **Automated backup ($50-100/month):** Set-it-and-forget-it data protection.
4. **Security monitoring ($100-200/month):** Professional oversight when you're ready.

Summing it all up

We hope this eBook has shown you that effective cybersecurity doesn't require a massive budget. By implementing free tools, following best practices, and training your team, you can significantly reduce your risk without breaking the bank.

Remember: Some protection is always better than no protection. Start where you are, use what you have, and build from there. Every step you take makes your business a harder target and reduces your risk.

The cybercriminals are counting on small businesses to remain easy targets. Prove them wrong—starting today.

If you'd like an experienced guide to assist you with your business's security planning—someone who can provide personalized advice based on your specific situation—and would prefer to work with a trusted advisor, we're ready to help.

Just click the GET IN TOUCH button and complete the brief form or give us a call. We look forward to hearing from you!