BROADVIEW TECHNOLOGY SOLUTIONS

Presents

The Minnesota Small Business

IT Survival Guide

Because Your Business Shouldn’t Freeze Up
Faster Than a Minneapolis Parking Lot in January

broadviewtech.com • Eden Prairie, MN • 612-276-2308

HELLO, FELLOW MINNESOTAN!

You've started (or are running) a small business. You've survived the -30F winters, the Vikings losing streaks, and the roundabout at Flying Cloud Drive. You're tough.

But your IT setup? That might be a different story.

The good news: you don't need a full-time IT department to keep your technology running smoothly. You just need the right foundation. That's exactly what this guide covers — in plain English, without the tech-bro jargon.

We're Broadview Tech, a local IT support company right in Eden Prairie. We work exclusively with small businesses in the Minneapolis-St. Paul metro area. This guide is our way of helping you understand what your business really needs — and what happens when you ignore it.

> *This guide covers five essential IT pillars every Minnesota small business should have in place: Backups, Endpoint Security, Wi-Fi & Network Security, Hardware Basics, and Knowing When to Call a Pro.*

SECTION 1: BACKUPS — YOUR BUSINESS'S INSURANCE POLICY

Imagine this: it's a Tuesday morning. You show up to work, coffee in hand, ready to tackle the day. You open your laptop and… nothing. The hard drive died overnight. Your QuickBooks files, your client list, your invoices, your contracts — all of it, gone.

Now imagine the same scenario, but this time you had a backup. You're back up and running within an hour or two. That's the difference between a rough Tuesday and a business-ending disaster.

What You Need:

- Cloud backup for all business-critical data (files, databases, email)
- At least, weekly automated backups — "manual" backups don't get done consistently
- Offsite backup: if your backup drive lives next to your computer, a fire or flood takes both
- Test your restores at least quarterly — a backup you've never tested is just a rumor

> **PRO TIP:** The 3-2-1 Backup Rule: Keep 3 copies of your data, on 2 different media types, with 1 copy offsite (i.e., in the cloud). This is the gold standard for small business backup.

What Happens Without It:

- The average cost of a data breach for a small business: $4,700+
- 60% of small businesses that lose critical data shut down within 6 months
- Ransomware attackers specifically target businesses without solid backups

Bottom line: cloud backup is the single most important investment you can make in your business's continuity. It costs less per month than a tank of gas, and it could save your business.

SECTION 2: ENDPOINT SECURITY — DON'T BE THE EASY TARGET

Cybercriminals aren't just targeting Fortune 500 companies. In fact, small businesses are their favorite targets — because small businesses often have weak (or no) defenses, but still have money, client data, and banking credentials worth stealing.

Endpoint security means protecting every device that connects to your business network or accesses your business data: computers, laptops, and yes, even smartphones.

What You Need:

- Business-grade antivirus/endpoint protection on every workstation and laptop
- Centrally managed security so you're not relying on each employee to keep their software updated
- Automatic threat detection and real-time response — not just signature-based virus scans
- Patch management: keeping Windows and software up-to-date is one of the most effective defenses

PRO TIP: Free antivirus is not enough for a business. Consumer-grade tools lack the centralized management, reporting, and threat intelligence that business environments need. If a breach happens and you were using free software, your cyber insurance may not cover it.

Warning Signs You're Under-Protected:

- You're still running Windows 10 (end of life: October 2025)
- Different employees have different antivirus software (or none)
- You haven't updated Windows in months
- You're relying on the free antivirus that came with the computer

SECTION 3: WI-FI & NETWORK SECURITY — LOCK THE DIGITAL DOOR

Your Wi-Fi is the front door to your entire business network. If it’s wide open, everything behind it is at risk — your computers, your files, your printers, your security cameras, and any smart devices.

What You Need:

- A business-grade router (not a $40 consumer router from Best Buy)
- Separate guest Wi-Fi network for customers and visitors — never share your main business network
- WPA3 encryption (or at minimum WPA2) — if you’re still on WEP, call us immediately
- A unique, strong password for your router admin panel (not the factory default)
- Firewall enabled and properly configured

> **PRO TIP:** Change your Wi-Fi password at least once a year, and immediately whenever an employee leaves. Former employees with Wi-Fi access are a surprisingly common source of business data incidents.

Bonus: Password Hygiene

- Use a business password manager (1Password, Bitwarden for Business) so employees aren’t using “Password1!” for everything
- Enable multi-factor authentication (MFA) on every business account: email, banking, cloud apps
- Never reuse passwords across business accounts

SECTION 4: HARDWARE BASICS — WHEN GOOD COMPUTERS GO BAD

Minnesota weather is hard on cars, roofs, and apparently also computers. Heat, cold, power surges, and age all take their toll. Here’s what you need to know to keep your hardware from failing at the worst possible moment (which is always a moment you can’t afford).

Hardware Lifespan Guidelines:

- Workstations & laptops: plan to replace every 4-5 years. Older machines cost more in lost productivity and IT support than a new one would.
- Network equipment (routers, switches): replace every 5-7 years, or when firmware updates end
- UPS (Uninterruptible Power Supply): every workstation should have one. Power surges and outages are the #1 cause of sudden hardware failure in the Midwest.

PRO TIP: A UPS is not just a battery backup — it's a surge protector that can prevent thousands of dollars in damage during a storm. Given Minnesota's love of dramatic weather, this is not optional.

Signs It's Time for New Hardware:

- Computer takes more than 2 minutes to boot up
- Employees complain about slowness daily
- The machine runs hot or the fan is constantly loud
- It's running Windows 10 or older
- You've had it repaired more than twice

SECTION 5: KNOW WHEN TO CALL A PRO

There's no shame in fixing things yourself — Minnesotans are famously self-reliant. But there's a difference between "I can change my own oil" and "I can rebuild a transmission." Your IT is the same way.

DIY is Fine For:

- Restarting your router when the internet drops
- Reconnecting a printer that went offline
- Basic software installs from trusted vendors
- Changing passwords

Call a Pro For:

- Any suspected virus, ransomware, or security incident — the first 30 minutes matter enormously
- Setting up your network, firewall, or new workstations
- Moving from consumer software to business-grade tools
- Anything that's been "strange" for a while and you've been ignoring it
- Planning your IT infrastructure as you grow

PRO TIP: A managed IT services contract gives you a dedicated local tech team for a flat monthly fee. For most businesses with 5-25 employees, it's significantly cheaper than hiring in-house, and you get better expertise and faster response times.

Ready to Stop Worrying About IT?

Broadview Tech offers managed IT services, cloud backup, and endpoint security for small businesses across the Minneapolis-St. Paul metro. We respond to emergencies within 30 minutes — because your business doesn't have time to wait.

broadviewtech.com • Eden Prairie, MN