FROM THE MEHRUTHERM BLOG · CYBERSECURITY

Cybersecurity Basics Every Small Business and Town Should Have

You do not need an enterprise budget to be reasonably safe. Here are the practical safeguards that stop most common cyber incidents, in plain language.

Himanshu Mehru · Founder, Mehrutherm

June 19, 2026

Many small businesses and local governments assume they are too small to attract cybercriminals.

Unfortunately, the opposite is often true.

Attackers favor smaller organizations precisely because they tend to have fewer defenses, limited IT resources, and fewer formal security habits. It is rarely personal. Automated tools scan the whole internet looking for easy ways in, and an office with no protection looks easy. The encouraging news is that you do not need an enterprise-sized budget to be a hard target. A handful of practical safeguards prevents the large majority of common incidents.

KEY TAKEAWAYS

- **Turn on multi-factor logins** for email and key systems.
- **Keep tested backups**, with at least one copy stored separately.
- **Install updates** so known security holes get closed.
- **Teach your team** to recognize a suspicious email.
- **Limit access** to what each person actually needs.

The Basics That Matter Most

Use Strong Passwords and Enable Multi-Factor Authentication

Most security breaches are not the result of sophisticated hacking. They start with a stolen, reused, or guessed password.

Adding multi-factor authentication (MFA) requires a second form of verification, such as a code from your phone, so a stolen password alone is not enough to get in. If you do only one thing this year, make it this, starting with your email accounts, since email is usually the master key to everything else.

Maintain Backups, and Test Them

Ask yourself a simple question: if your files disappeared tomorrow, how quickly could you recover?

Effective backups follow a simple rule of thumb: more than one copy, on more than one kind of storage, with at least one copy kept off-site or in the cloud. Just as important, test a restore now and then. A backup nobody has ever restored is an assumption, not a recovery plan, and ransomware is a lot less frightening when you can simply roll back.

Keep Systems and Software Updated

Many attacks exploit known weaknesses that already have fixes available. The fix exists; it just has not been installed.

Letting your computers, phones, and software apply their updates closes those doors before someone walks through them. It is dull work, which is exactly why it gets skipped, and exactly why attackers count on it.

Train People to Spot Suspicious Emails

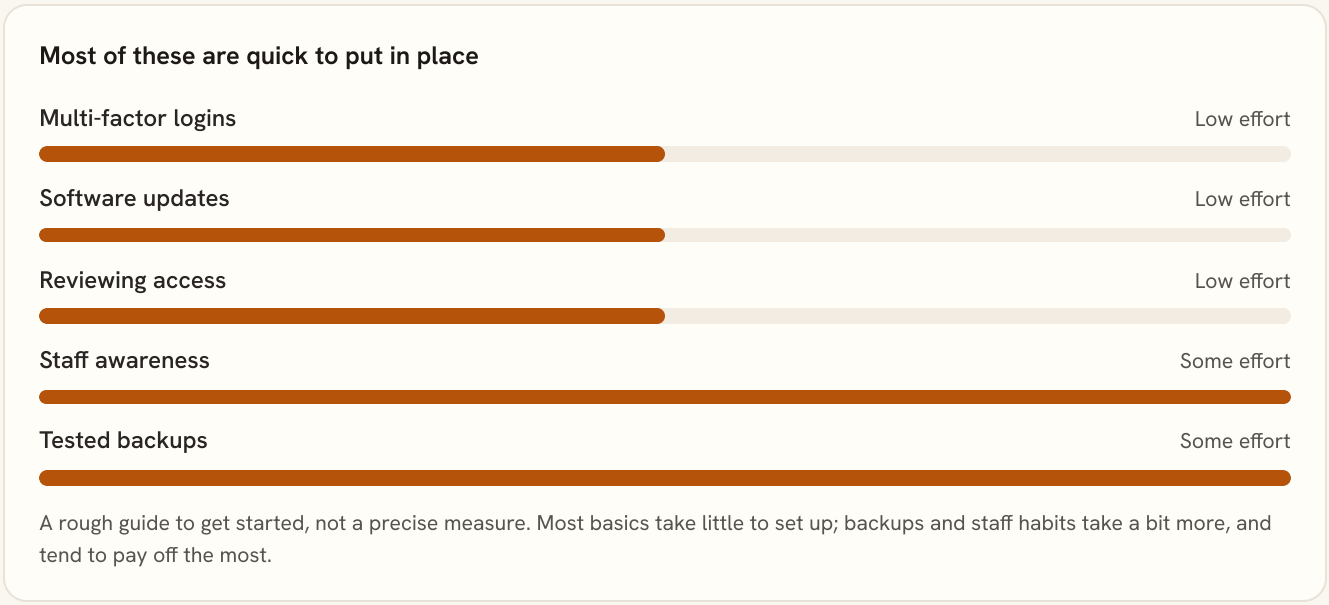
Phishing remains one of the most common ways trouble gets in. A convincing email can fool even a careful person into clicking a bad link or opening an infected attachment.

You do not need formal training programs. A short, plain conversation about what to watch for, and a clear "when in doubt, ask before you click" rule, prevents most of it.

Review Access Regularly

Not everyone needs access to everything. People should have the access their job requires and no more, and when someone leaves, their access should leave with them the same day.

Fewer open doors means fewer ways in, and far less damage if any single account is ever compromised.



Why Towns Have an Extra Reason to Care

For local governments, cybersecurity is about more than avoiding disruption.

Insurers, state agencies, and risk pools increasingly expect a baseline of security to be in place, and coming up short can affect your coverage, your premiums, and your grant eligibility. If your town carries cyber insurance, this is worth understanding closely. We cover it in detail in what your insurer now expects.

Protecting systems and resident information is not just a technical task. It is part of good governance, and increasingly, part of staying insured.

THE MOST EXPENSIVE BOX YOU'LL EVER CHECK

On an insurance questionnaire it is tempting to check every box. But if a control is not actually in place and you later file a claim, that gap can come back to bite you, exactly when you need the coverage most. Make the boxes true before you check them.

You Do Not Have to Do This Alone

Putting these fundamentals in place does not require a large IT department. It takes the right setup once, and someone keeping a quiet eye on it after that.

That is a big part of what we do for the businesses and towns we look after: the protections run in the background, the backups get tested, the updates get applied, and we are the ones watching. If you are unsure how your organization measures up, now is the best time to find out. A simple review today can prevent a far more expensive conversation tomorrow.

MEHRUTHERM · CRESTON, WA

Want to know where you stand? Get in touch for a cybersecurity review and practical, plain-English recommendations for your organization.

mehrutherm.com/quote