PINNACLE ACCESS INC.

The Business Owner's Guide to

Cybersecurity in 2026

7 Things You Must Do to Protect Your Business

Cybercrime costs businesses billions every year — and the #1 target is no longer large corporations. It's businesses like yours. This guide gives you the 7 essential steps every business owner must take in 2026 to stay secure, protect client data, and avoid costly downtime.

Pinnacle Access Inc.
IT Services & Cybersecurity | San Diego, CA
619-282-7596 | pinnacleaccess.net

Why Cybersecurity Can't Wait

The threat landscape has changed dramatically. Hackers no longer just target Fortune 500 companies — they specifically target businesses with 10 to 100 employees because they know these organizations typically have valuable data but limited IT security resources.

Consider these facts: The average cost of a data breach for a small business is over $200,000. 60% of small businesses that suffer a cyberattack close within 6 months. And the average breach goes undetected for 241 days — meaning by the time you know you've been hacked, the damage is already done.

The good news? You don't need a massive IT budget to protect your business. The 7 steps in this guide are practical, affordable, and proven to dramatically reduce your risk. Let's get started.

STEP 1 OF 7

Enable Multi-Factor Authentication (MFA) on Everything

Passwords alone are no longer enough. When an employee's password is stolen — through phishing, a data breach, or a weak password — MFA is the last line of defense that stops an attacker from getting in. MFA requires a second form of verification (a phone app, text code, or hardware key) in addition to a password.

- → Enable MFA on Microsoft 365, email, and any cloud applications immediately
- → Use an authenticator app (Microsoft Authenticator, Duo) — not SMS text codes which can be intercepted
- → Require MFA for all employees — not just administrators
- → Consider phishing-resistant MFA (FIDO2 keys) for your most sensitive accounts

> ***Quick Win:*** *Enabling MFA on Microsoft 365 alone blocks over 99% of automated account compromise attacks.*

STEP 2 OF 7

Keep All Software and Systems Updated

Outdated software is one of the most common entry points for hackers. When vendors release security patches, they are often responding to known vulnerabilities that attackers are already actively exploiting. Every day you delay an update is a day you're exposed.

- → Enable automatic updates for Windows, macOS, and all applications
- → Patch servers and network equipment on a regular schedule — don't delay
- → Replace end-of-life systems that no longer receive security updates (Windows Server 2012, Windows 10)
- → Include third-party software like browsers, Adobe, and Java in your patch management

> ***Quick Win:*** *Create a monthly 'patch day' — schedule 2 hours the first Tuesday of every month to review and apply updates.*

STEP 3 OF 7

Back Up Your Data — And Test Your Backups

Ransomware attacks encrypt your files and demand payment to restore them. The only guaranteed defense is a clean, tested backup that attackers cannot reach. Many businesses think they have a backup — until they need it and discover it hasn't been working for months.

→ Follow the 3-2-1 rule: 3 copies of data, on 2 different media types, with 1 stored offsite

→ Back up to a location that is isolated from your main network — ransomware can encrypt network shares

→ Include Microsoft 365 email and data in your backup — Microsoft does NOT guarantee data recovery

→ Test your backup restoration at least quarterly — a backup you've never tested is not a backup

Quick Win: *Ask your IT provider: 'When did we last successfully restore from backup?' If they can't answer, that's a problem.*

STEP 4 OF 7

Train Your Employees — They Are Your Biggest Risk

Over 90% of cyberattacks start with a phishing email. Your employees are clicking on links, opening attachments, and entering credentials every day. Without training, one wrong click can give an attacker full access to your network. Security awareness training turns your employees from a liability into a first line of defense.

→ Conduct security awareness training at least twice a year for all staff

→ Run simulated phishing tests — send fake phishing emails to employees to see who clicks

→ Train employees to recognize social engineering: urgency, authority, and fear are red flags

→ Create a clear process for reporting suspicious emails — make it easy and blame-free

Quick Win: *Most cyber insurance providers now require documented security awareness training. It can lower your premiums.*

STEP 5 OF 7

Secure Your Email with Advanced Filtering

Email is the #1 attack vector for businesses. Phishing, malware attachments, business email compromise (BEC), and spam are constant threats. Basic email providers include basic spam filters — but advanced threats require advanced filtering that analyzes email content, sender reputation, and attachment behavior.

→ Deploy an enterprise email security solution beyond basic spam filtering

→ Enable attachment sandboxing — suspicious files are detonated in a safe environment before delivery

→ Configure DMARC, DKIM, and SPF records to prevent email spoofing of your domain

→ Be especially cautious of wire transfer requests or changes to payment details received via email

> ***Quick Win:*** *Business Email Compromise (BEC) costs businesses more than ransomware. Always verify financial requests by phone.*

STEP 6 OF 7

Control Who Has Access to What

Not every employee needs access to everything. The principle of least privilege means giving users only the access they need to do their job — nothing more. This limits the damage an attacker can do if they compromise one account, and reduces the risk from insider threats.

→ Audit user accounts and permissions at least twice a year — remove access for former employees immediately

→ Use separate admin accounts for IT tasks — never browse the web or check email with an admin account

→ Implement role-based access control (RBAC) in Microsoft 365 and your line-of-business applications

→ Disable or delete accounts within 24 hours of an employee leaving the company

> ***Quick Win:*** *Former employee accounts left active are one of the most common causes of data breaches. Offboarding checklists save businesses.*

STEP 7 OF 7

Have an Incident Response Plan

Despite your best efforts, a security incident may still occur. The difference between a minor disruption and a catastrophic breach often comes down to how quickly and effectively you respond. Businesses with an incident response plan recover faster and suffer less financial damage.

→ Document who to call when something goes wrong: IT provider, cyber insurance, legal counsel

- → Know how to isolate an infected computer from your network immediately — disconnect ethernet and Wi-Fi
- → Do NOT pay ransomware demands without consulting your IT provider and legal counsel first
- → Report breaches to your cyber insurance provider within the required timeframe — delays can void coverage

Quick Win: *Ask your IT provider for a one-page incident response card. Post it near workstations so staff know what to do.*

Your Next Step

How many of these 7 steps does your business currently have in place? If you're unsure — or if you know there are gaps — now is the time to act. Cybercriminals are not waiting.

Pinnacle Access Inc. provides managed IT services and cybersecurity for businesses in San Diego. We can assess your current security posture, identify gaps, and implement the protections you need — at a predictable flat-rate cost with no surprises.

Ready to protect your business?

Call us today for a no-obligation conversation about your IT security.

■ **619-282-7596**

■ pinnacleaccess.net

■ 3435 Camino Del Rio South, Suite 316, San Diego, CA 92108

This guide is provided for informational purposes only. Pinnacle Access Inc. recommends working with a qualified IT professional to assess and implement security measures appropriate for your specific business environment.