Build Your Human Firewall - One Smart Step at a Time

Why This Roadmap Exists

Cybersecurity doesn't fail because businesses don't care — it fails because it feels overwhelming.

This roadmap breaks cybersecurity into **12 vital actions**, one per month. Each step is practical, achievable, and proven to reduce real-world risk for small businesses.

Think of this as **building a Human Firewall** — strong people, supported by smart technology, making safer decisions every day.

Be a Human Firewall

Technology alone can't stop cybercrime.

A **Human Firewall** is built when you:

- Question unexpected logins
- Pause before entering credentials
- Expect MFA prompts — and report unusual ones

ACT SMART I.T.
Helping You Benefit From Today's Technologies

332 Main Street, Wareham, MA 02571
781-826-9665 | 855-WOW-SERVICE
ACTSmartIT.com

January's Tip -
Set up MFA Everywhere!
#1 SET UP MFA EVERYWHERE!
Two-Factor Authentication
January To-Do List
1. Set up MFA everywhere! ✓

Our 12 Month Cybersecurity Roadmap

Follow us each month at:
https://actsmartit.com/2026-cybersecurity-roadmap/

The #1 Most Important Cybersecurity Action:

January: Turn On Multi-Factor Authentication (MFA) Everywhere

Why This Matters

Most cyberattacks don't start with hackers breaking in — they start with **stolen passwords**.

Passwords are easy to steal through phishing emails, fake login pages, or data breaches. Once attackers have a password, they can walk right in.

Multi-Factor Authentication (MFA) stops them.

What Is MFA?

MFA means you need **more than just a password** to log in.
It usually combines:

- **Something you know** – your password

- **Something you have** – a phone app, code, or security prompt

Even if a criminal steals your password, they **can't get in without the second step**.

Think of MFA like a **deadbolt on your door**.
A password alone is like a simple lock. MFA adds a second layer of protection.

If your business only completes one cybersecurity task this year, this should be it.

Where MFA Should Be Enabled First

Start with the systems that matter most:

- **Email accounts** (Microsoft 365, Google Workspace)
- **Remote access** (VPNs, remote desktop tools)
- **Financial systems** (banking, payroll, QuickBooks)
- **Admin and owner accounts** (highest priority)

Once those are protected, roll MFA out to **all employees**. Then roll MFA out to **all users**.

Common MFA Myths (and the Truth)

"MFA is too annoying."
It takes seconds — recovering from a breach takes months.

"We're too small to be targeted."
Small businesses are targeted *more* because they're easier.

"MFA won't stop everything."
Correct — but it stops the most common and damaging attacks.

A Human Firewall Moment

Technology alone isn't enough. Employees play a huge role in security.

Human Firewall Rule #1:
If you didn't try to log in, don't approve the MFA request.

Unexpected MFA prompts should be reported right away. That could be a sign someone already has your password.

January Takeaway

- Passwords alone are no longer enough.

- Adding MFA is one small step that makes a **huge difference**. It protects your data, your money, your reputation, and your business.

- This January, turn on MFA — and start the year with stronger security.