Small-Business Ransomware Checklist

14 plain-language steps from Blueprint Basics: A Small Business Guide to Ransomware Defense. You don't need a technical background — start with the three below, then work down the list.

START HERE — DO THESE 3 FIRST

1 **Turn on multi-factor authentication (MFA) — start with your email** even if a password is stolen, MFA keeps attackers out.

2 **Back up your data — and test the restore** so you can recover without paying.

3 **Keep your software updated** closes the most common way in.

Next best thing: train your team to spot phishing — 30 minutes a year.

→ **Where to turn on MFA:** your email provider's security settings, or find any service at **2fa.directory**

GOVERNANCE BASICS — WRITE IT DOWN

- ☐ Map your data: what you have, where it lives *3.1 · ~30 min*
- ☐ Setup checklist for new devices & network *4.1/4.2 · ~15 min/device*
- ☐ Process to grant & remove access *6.1/6.2 · ~15 min*
- ☐ Keep software updated (turn on auto-updates) *7.1/7.2 · ~10 min/mo*
- ☐ Know where your activity logs are *8.1 · ~20 min*
- ☐ Written data-recovery plan — and test it *11.1 · ~1 hr*
- ☐ Train your team on phishing, once a year *14.1 · ~30 min/yr*
- ☐ One-page incident “break-glass” plan *17.3 · ~30 min*

KNOW YOUR ENVIRONMENT

- ☐ List every device your business uses *1.1 · ~30 min*
- ☐ List approved software + MFA per app *2.1 · ~20 min*
- ☐ List every account + turn on MFA *5.1 · ~30 min*

YOUR 3 TOOLS (FREE DOWNLOADS)

- Cybersecurity Starter Inventory (a spreadsheet, prefilled)
- Blueprint Basics Starter Templates (checklists → incident plan)
- Questions to bring to your IT provider (MSP)

GO FURTHER (FREE)

CISA #StopRansomware cisa.gov/stopransomware

FBI — report an attack ic3.gov

Global Cyber Alliance Toolkit gcatoolkit.org