NAPLES COMPUTERS HOW-TO · SECURITY & SAFETY

Backups for Business: What Ransomware-Proof Really Means

A live cloud sync feels like a backup, but ransomware can encrypt and upload the damage right along with it. This guide covers what actually protects a business backup from ransomware: offline copies, immutable storage, and tested restores.

The myth worth clearing up

A sync isn't the same thing as a safe copy.

"I sync to the cloud" isn't enough
If ransomware encrypts your files, a live sync can upload the encrypted version, too.

Ransomware looks for backups
Many variants actively search for connected backups, and delete or encrypt them.

What actually protects you
Copies it genuinely can't reach, or can't alter, even once it's inside.

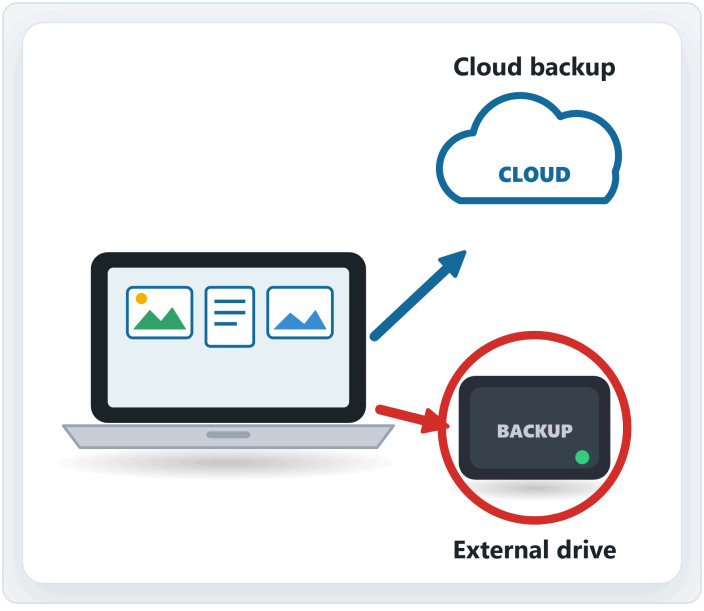
What actually makes a business backup ransomware-proof

OFFLINE COPIES

1 Keep at least one copy offline

A drive that's disconnected when it's not actively backing up can't be reached by ransomware at all.

WHAT TO DO
Rotate it, or use a backup appliance that disconnects itself automatically between jobs.



IMMUTABLE COPIES

2 Immutable: can't be changed, not even by an admin

Some cloud backup services offer storage that can't be altered or deleted for a set period of time.

WHAT TO DO

Use it with caution, it doesn't meet every compliance requirement, and misconfiguring it gets expensive.



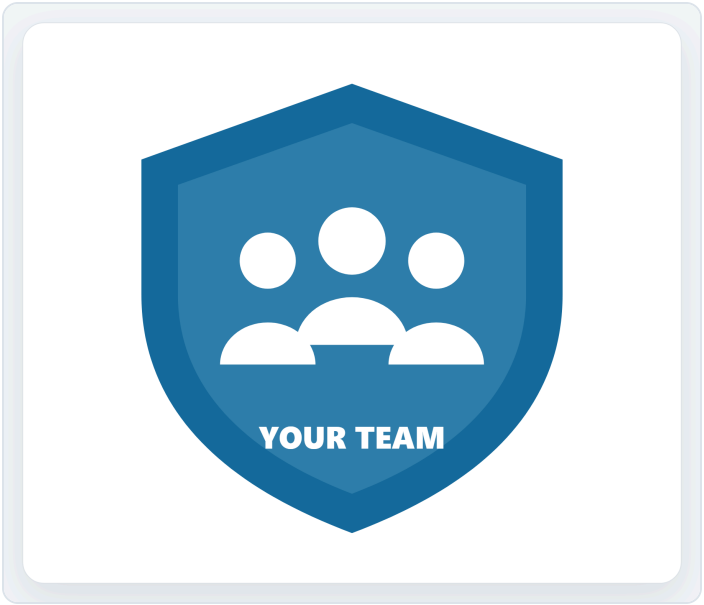
NAPLES COMPUTERS

★ Is your business backup actually ransomware-proof?

We'll review your setup, test a restore, and add offline or immutable protection if it's missing.

WHAT TO DO

Call 239-513-1960, before you need to find out the hard way.



A backup you haven't tested isn't proven

- [ ] **Test a full restore regularly**
  Not just that the backup ran, that you can actually get the data back
- [ ] **Keep “golden images” ready**
  A preconfigured, rebuildable template gets a system running again faster
- [ ] **Keep a hard copy of your response plan**
  If your network is down, you need the plan even without it

The rule, updated for ransomware

- [ ] **3 copies, on 2 different kinds of media**
  The classic 3-2-1 rule still applies, as a starting point
- [ ] **1 copy offsite**
  A fire, flood, or theft shouldn't be able to take out every copy at once
- [ ] **At least 1 copy offline or immutable**
  The part that specifically protects you against ransomware

Recap: ransomware-proof backups

- [ ] A live sync alone isn't a ransomware-proof backup
- [ ] Keep at least one copy genuinely offline
- [ ] Immutable storage can't be changed, not even by an admin
- [ ] Test full restores regularly, and keep golden images ready
- [ ] Not sure if yours qualifies? Call Naples Computers

Test a full restore regularly, not just whether the backup job ran. A backup you've never actually restored from isn't proven to work when you need it.

NAPLES COMPUTERS

Not sure if your backup is actually ransomware-proof? We'll check it.

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**