LESSON 04 OF 05 · 8 MIN · ESSENTIAL

Backups that actually work

Cloud sync is not a backup. Learn the 3-2-1 pattern, protect the backup from ransomware, and prove it works.

Sync is not backup

If you delete a file and it disappears from every device, that's sync. If ransomware encrypts your laptop and the encrypted versions replicate to the cloud folder, that's sync too. Sync is excellent for working across devices and useless as a recovery plan.

A backup is a separate copy you can go back to, with a history long enough that you notice the problem before it expires.

3-2-1, in plain terms

- **Three copies:** the live data plus two backups.
- **Two media:** for example cloud storage plus a local drive or NAS.
- **One offline or immutable:** disconnected, or locked so it can't be altered for a retention period.

Cover email, finance, customer records, payroll and the files people actually use, not just the shared drive. Use a separate backup account with MFA. Turn on version history and alerting for failures and mass deletion.

The ransomware test

Ask: if an attacker had my normal admin account right now, could they delete every backup? If yes, you don't yet have ransomware-resistant backups. Offline drives, object lock, immutable snapshots and separate credentials are the answer.

Then restore a real file. An untested backup is a hope with a retention policy.

THE DETAIL THAT MATTERS

A nightly backup to a folder the ransomware can also reach is not a backup strategy. One copy must be out of reach of the account that runs your business.

Key takeaways

- ✓ Cloud sync replicates deletions and encryption ; it is not a backup.
- ✓ Three copies, two media, one offline or immutable.
- ✓ Protect the backup account with MFA and separate credentials.
- ✓ Test a restore before you need one.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.