LESSON 03 OF 04 · 6 MIN · ESSENTIAL

Restore drills that prove it works

A backup is a claim. A restore is evidence. Here's the twenty-minute drill.

The only test that counts

Restoring a file you created five minutes ago proves nothing. Choose something real (last month's invoices, a customer contract, the accounts file) and restore it to a different location. Time it. Open it. Check it's the version you expected.

Do this twice a year, and after changing backup tools or providers.

Record the result

Keep a simple log: date, what was restored, who did it, how long it took, whether it worked, and what was fixed. This is useful operationally and increasingly requested by insurers.

If it failed, fix it that week and repeat. A failed restore discovered in a drill is a gift; discovered during ransomware, it is a catastrophe.

Once a year, go further

Walk through a fuller scenario: a lost laptop, a deleted mailbox, a server that won't start. Who would do the work? How long would it take? What would the business do meanwhile? A tabletop conversation with the right people exposes most gaps without the cost of a full simulation.

> **WATCH THEM DO IT**
>
> If a provider manages your backups, ask them to demonstrate a restore while you watch. A report saying “backups are healthy” is not the same as recovering your data.

Key takeaways

- ✓ Restore a real file, not a test file.
- ✓ Time it and record the result.
- ✓ Repeat twice a year and after tooling changes.
- ✓ Walk through a fuller recovery annually.

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