Respond To A Ransomware Attack On A Small Business

Plain-English how-to. ~First 72 hours playbook. Step-by-step under pressure.

The first-72-hours playbook for ransomware response in a small business.
Print, share, and re-run quarterly.

Do This Right Now

#	STEP
1.	Isolate (unplug). Do NOT shut down.
2.	Photograph ransom note. Document everything.
3.	Call cyber insurance, IT provider, attorney.
4.	Report to FBI via ic3.gov within 24 hours.
5.	Check nomoreransom.org for free decryption.
6.	Attempt recovery from backups before considering payment.
7.	Rebuild from clean media; rotate all credentials.
8.	Notify customers per legal counsel; run post-incident review.

Why This Matters

- Ransomware is the most likely catastrophic cyber event for a small business. The combination of encrypted files, threatened data leak
- Prepared organizations recover. Unprepared organizations pay ransoms (often without getting decryption) and still fail. The FBI strong
- Most ransomware incidents follow a predictable pattern: initial access via phishing or RDP, dwell time of days to weeks while attackers