CI/CD Common Pitfalls (for Small Teams)

Real-world gotchas and how to avoid them.

1. Treating CI Logs as an Afterthought

- Symptom: 'It works locally' but the pipeline fails with cryptic errors.
- Fix: Make logs first-class. Pipe test output to files, upload as artifacts, and keep timestamps.
- Tip: Add `set -euo pipefail` to shell scripts to fail fast and loudly.

```
set -euo pipefail
echo "Starting build at $(date -Iseconds)"
# your build steps here
```

2. Secrets in Plain Text

- Symptom: Passwords or keys appear in YAML or code.
- Fix: Use the platform's secrets store (GitHub/Azure/GitLab/Bitbucket) or a cloud secret manager (AWS SSM, Azure Key Vault, GCP Secret Manager).
- Tip: Use environment injection and never echo variables (use `set +x` around sensitive commands).

```
set +x
export DB_PASSWORD="$PROD_DB_PASSWORD"
set -x
# run commands that don't print secrets
```

3. Deploying Without a Health Check

- Symptom: Green pipeline, broken site.
- Fix: Add a `/health` endpoint and curl it after deploy; fail the job if it returns non-200.

```
curl -fsS https://example.com/health || { echo "Health check failed"; exit 1; }
```

4. One Big Pipeline for Everything

- Symptom: Slow, flaky pipeline blocks all work.
- Fix: Split into jobs (build, unit tests, integration tests, deploy) with caching and conditional execution.

5. No Rollback Strategy

- Symptom: Emergency hotfixes take hours.
- Fix: Keep N previous artifacts, automate rollback, and prefer blue/green or deploy slots when available.

6. Ignoring Infrastructure Drift

- Symptom: Snowflake servers behave differently than staging.
- Fix: Use IaC (Terraform/CloudFormation/Bicep) and keep it in the repo.

7. Skipping Linting/Unit Tests 'for Speed'

- Symptom: Time saved now, time lost later.
- Fix: Add lightweight lint/test steps with caching so they're fast.

8. Over-Privileged IAM Roles

- Symptom: `*:*` permissions everywhere.
- Fix: Apply least privilege and scope roles to specific buckets, apps, and services.

9. Missing Branch Protection

- Symptom: Force pushes to main break production.
- Fix: Require PRs, reviews, and passing checks before merge.

10. Not Budgeting for CI/CD

- Symptom: Surprise bills from runners, storage, egress.
- Fix: Set limits/quotas, measure usage, and enforce caching/artifact retention policies.