Secrets

Computing

Where credentials must not go, and what to do when one leaks.

Practices that prevent the majority of credential leaks.

Never

- Commit secrets to a repository
- Put them in front-end code
- Log them, even at debug level
- Email or paste them into chat
- Share one key across environments

Instead

- Environment variables or a secret manager
- .env in .gitignore, .env.example committed
- Separate keys per environment
- Least privilege scope per key
- Automatic rotation where possible

When one leaks

- Revoke first, investigate after
- Rotate everything it could reach
- Check the access logs
- Rewriting git history does not un-leak it

> Public repositories are scanned continuously. A committed key is typically abused within minutes, not days.