> **It is never too late to be what you might have been.**
>
> **- George Eliot**

---

1. **Two-Factor Authentication (2FA)**
    - Require all users to have a 2fa on their accounts
        - as it adds an extra layer of security by requiring a second verification in addition to the password
    - Use hardware security keys
        - these are immune to phishing attacks, making them the most secure 2fa
2. **Repository Permissions**
    - limit repo access
        - this limits unauthorized changes
    - use teams for permission mgt
        - private repo -- only those with access can view it
        - Base role --
        - direct access --
        - ie. create teams in your organization and assign them repos because it makes it easier to manage permissions at scale
3. **Branch Protection**
    - set branches rules that prevent direct pushes to important branches like main i.e branch protection rules
    - you may also require status checks to pass before merging by ensuring that all tests pass before code is merged.
4. **Code Reviews**
    - Enable github secret scanning by enabling pull request reviews before merging as code reviews catch vulnerabilities that automated tests might miss.
5. **Secret Scanning**
    - Enable github secret scanning

        - this helps to identify exposed secrets like API keys in your code.

6. **Dependency Scanning**
    - Use the Dependabot as dependabots scan your dependencies for known vulnerabilities and suggests fixes.
7. **Audit Logs**
    - Audit logs provide a history of all actions taken in your repository, helping you spot any unauthorized or suspicious activity.
8. **GitHub Actions Security**
    - Limit permissions for github actions by using the permissions key in your workflow YAML file.
    - This restricts the permissions of the GitHub token used during the workflow run.
9. **Third-Party Integrations**
    - Vet all third-party apps by reviewing the permissions requested by third-party apps before installing them because malicious apps can compromise your repository.
10. **Employee Training and Awareness**
    - Conduct Regular Security Training