1. В чем отличие github от git?

Git - это система контроля версий, работающая локально, а GitHub - веб-платформа для хостинга репозиториев Git и совместной разработки.

* 1. Что такое пуш(push) в github?

это операция, при которой локальные изменения в репозитории Git отправляются на удаленный репозиторий на GitHub. При выполнении команды "пуш" в Git, все коммиты, которые были сделаны локально, отправляются на сервер GitHub, где они становятся доступными для других разработчиков, работающих над проектом.

* 1. Что такое клон(clone) в github?

это создание локальной копии удаленного репозитория на вашем компьютере. Когда вы клонируете репозиторий, вы получаете все файлы, историю коммитов и ветки проекта.

* 1. Как защитить свой репозиторий на GitHub?

1. Приватные репозитории: Создайте приватный репозиторий, который будет видим только для вас или ограниченного круга сотрудников. В приватном репозитории все коммиты и изменения будут храниться в безопасности.

2. Двухфакторная аутентификация: Включите двухфакторную аутентификацию (2FA) для своей учетной записи GitHub. Это позволит вам использовать не только пароль, но и дополнительный способ подтверждения вашей личности, например, с помощью кода, который будет отправлен на ваш телефон или используя аутентификатор приложения.

3. Конфигурация доступов: Управляйте доступами к вашему репозиторию, чтобы ограничить права других пользователей, которые могут получить доступ к вашему коду. GitHub предоставляет различные роли доступа, такие как "Owner", "Collaborator", "Contributor" и другие. Настройте эти роли в соответствии с вашими потребностями в безопасности.

4. Используйте strong пароли: Убедитесь, что ваш пароль для GitHub является надежным и сложным, чтобы максимально защитить вашу учетную запись от взлома. Избегайте использования очевидных комбинаций и используйте комбинацию букв, цифр и специальных символов.

5. Регулярные резервные копии: Регулярно создавайте резервные копии вашего репозитория, чтобы предотвратить потерю данных. GitHub предоставляет собственные инструменты для создания резервных копий, а также есть возможность использовать сторонние инструменты для резервного копирования.

6. Аудит и мониторинг: Внимательно следите за активностью в вашем репозитории и проверяйте журналы коммитов и запросов на изменение. Если вам кажется, что произошли несанкционированные изменения или доступы, немедленно примите меры для защиты вашего репозитория.

Убедитесь, что вы принимаете все необходимые меры безопасности и следуете передовым практикам при работе с репозиториями на GitHub, чтобы максимально защитить свой код и данные.