Creating a strong password

Secure your account on GitHub.com with a strong and unique password using a password manager.

You must choose or generate a password for your account on GitHub.com that is at least:

- Eight characters long, if it includes a number and a lowercase letter, or
- 15 characters long with any combination of characters

To keep your account secure, we recommend you follow these best practices:

- Use a password manager to generate a password of at least 15 characters.
- Generate a unique password for GitHub. If you use your GitHub password elsewhere and that service is compromised, then attackers or other malicious actors could use that information to access your account on GitHub.com.
- Configure two-factor authentication for your personal account. For more information, see "About two-factor authentication."
- Optionally, add a passkey to your account to enable a secure, passwordless login. For more information, see "About passkeys" and "Managing your passkeys."
- Never share your password, even with a potential collaborator. Each person should use their own personal account on GitHub. For more information on ways to collaborate, see: "Inviting collaborators to a personal repository," "About collaborative development models," or "Collaborating with groups in organizations."

When you type a password to sign in, create an account, or change your password, GitHub will check if the password you entered is considered weak according to datasets like HaveIBeenPwned. The password may be identified as weak even if you have never used that password before.

GitHub only inspects the password at the time you type it, and never stores the password you entered in plaintext. For more information, see HaveIBeenPwned.

You can only use your password to log on to GitHub using your browser. When you authenticate to GitHub with other means, such as the command line or API, you should use other credentials. For more information, see "About authentication to GitHub."

When Git prompts you for your password, enter your personal access token. Alternatively, you can use a credential helper like Git Credential Manager. Password-based authentication for Git has been removed in favor of more secure authentication methods. For more information, see "Managing your personal access tokens."

Further reading

- "Caching your GitHub credentials in Git"
- "Keeping your account and data secure"