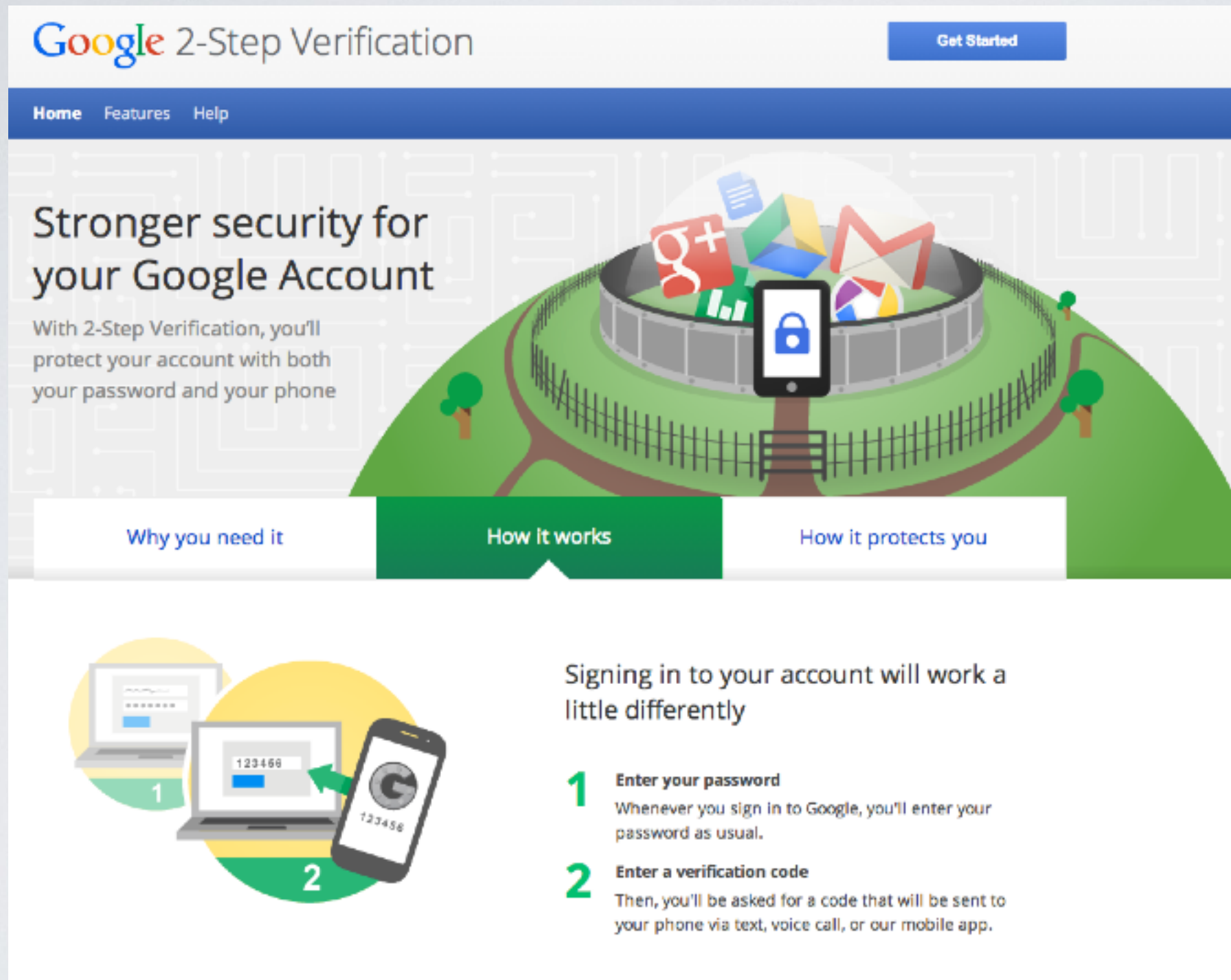


Example of two-factor authentication



The screenshot shows the Google 2-Step Verification landing page. At the top, the Google logo is followed by '2-Step Verification' and a 'Get Started' button. A navigation bar includes 'Home', 'Features', and 'Help'. The main heading is 'Stronger security for your Google Account', with a subtext: 'With 2-Step Verification, you'll protect your account with both your password and your phone'. Below this is a large illustration of a fortress with a smartphone as the entrance, surrounded by Google service icons. A tabbed interface shows 'How it works' as the active section. The content area explains the two-step process: 1. Enter your password, and 2. Enter a verification code sent to the phone. An illustration on the left shows a laptop screen with a password field and a smartphone displaying a verification code, with numbered circles 1 and 2 indicating the steps.

Google 2-Step Verification [Get Started](#)

[Home](#) [Features](#) [Help](#)

Stronger security for your Google Account

With 2-Step Verification, you'll protect your account with both your password and your phone

[Why you need it](#) **How it works** [How it protects you](#)

Signing in to your account will work a little differently

- 1 Enter your password**
Whenever you sign in to Google, you'll enter your password as usual.
- 2 Enter a verification code**
Then, you'll be asked for a code that will be sent to your phone via text, voice call, or our mobile app.

<https://twofactorauth.org/>

Choosing the authentication mechanism

- ➔ Driven by the risk analysis and the costs
How hard is it to?
 - Make you reveal your secret password
 - Duplicate a credit card
 - Fake your fingerprints
- ◎ There is no perfect authentication