M Gmail   **Frank Marchese <frankmarchese01@gmail.com>**

Fwd: Publicly Accessible Google API Key for Personal-Budget-PWA (id: personal-budget-pwa-5defb)

Frank Marchese <frankmarchese01@gmail.com>   Mon, Feb 2, 2026 at 11:47 PM
To: Things 3 To-do List <add-to-things-m13c6tgox4gybwz8r6192@things.email>

Sent from my iPhone

Begin forwarded message:

> **From:** noreply-google-cloud-compliance@google.com
> **Date:** February 2, 2026 at 11:31:23 PM EST
> **To:** frankmarchese01@gmail.com
> **Subject: Publicly Accessible Google API Key for Personal-Budget-PWA (id: personal-budget-pwa-5defb)**

Google Cloud Platform   **MY CONSOLE**

Suspicious Activity Alert

Publicly accessible Google API key for Google Cloud Platform project Personal-Budget-PWA (id: personal-budget-pwa-5defb)

Dear Customer,

We have detected a publicly accessible Google API key associated with the following Google Cloud Platform project:

Project Personal-Budget-PWA (id: personal-budget-pwa-5defb) with API key AIzaSyDwUA0paVI6n01aENV5Q2aLwVz1DEDtNuA

The key was found at the following URL: https://github.com/FrankM77/personal-budget-pwa/blob/f139dc18922b48ac6aa09342da2bacc8d2c87daf/assets/index-6KVI7PqI.js

For a subset of abuse issues, we send abuse notifications in log format. Please login to your console and review this abuse notification in Cloud Logging.

We believe that you or your organization may have inadvertently published the affected API key in public sources or on public websites (for example, credentials mistakenly uploaded to a service such as GitHub.)

Please note that as the project/account owner, you are responsible for securing your keys. Therefore, we recommend that you take the following steps to remedy this situation:

1. If this key is intended to be public (or if a publicly accessible key isn't preventable):
   - Log in to the Google Cloud Console and review the API and billing activity on your account, ensuring the usage is in line with what you expected.
   - Add API key restrictions to your API key, if applicable.
2. If this key was NOT meant to be public:
   - Regenerate the compromised API key: Search for Credentials in the cloud console platform, Edit the leaked key, and use the Regenerate Key button to rotate the key. For more details, review the instructions on handling compromised GCP credentials.
   - Take immediate steps to ensure that your API key(s) are not embedded in public source code systems, stored in download directories, or unintentionally shared in other ways.
   - Add API key restrictions to your API key, if applicable.

The security of your Google Cloud Platform account(s) is important to us. To learn more about how to respond to abuse notifications and warnings, click here.

<div align="center">

GO TO MY CONSOLE

</div>

Sincerely,

Google Cloud Platform Trust & Safety

<div align="center">

Google

© 2019 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043

</div>

You have received this mandatory service announcement to update you about important changes
to Google Cloud Platform or your account.