How can I keep my OpenAI accounts secure?

Protect your account from fraud with these best practices.

Updated over 10 months ago

Table of contents

Contact us right away if you're concerned that your account or API key has been compromised. You can reach out to the OpenAI support team by opening a new chat in the bottom right corner of any Help Center page. We're here to help.

Introduction

When using OpenAI services, it's crucial to keep both your API key and account secure. Protect yourself from API key leaks and account takeovers with these best practices.

Understanding API Key leaks

An API key is essentially your personalized access code to use the OpenAI API. If this key gets leaked, unauthorized users could access the API using your account resulting in unauthorized charges or your account being used to violate our terms of service.

How to prevent leaks

1. **Use environment variables**

- Store your API key in environment variables within your development environment.
- This ensures the key is not hard-coded into your application, making it less likely to be exposed.
- If you're using GitHub Actions, use GitHub secrets to keep your API key secure.

2. **Be cautious when using third-party products**
   - Exercise caution when using third-party libraries, frameworks, or tools that request access to your API key. Even though a product may seem reputable, there's always the risk of key exposure or misuse.
   - Before using a third-party product that requires your API key, thoroughly research the company and the product. Check reviews, read their privacy policy, and see if the community has raised any security concerns.
3. **Set reasonable spend limits**
   - Set your monthly budget to a value near to your expected spend. This means that, if your key does leak, the amount of authorized spend will be lower.
   - You can can change your limits via the limits dashboard.
4. **Don't ship your API key**
   - It can be tempted to ship your API key embedded as part of an application to avoid running a server for a mobile app, for example. However, this makes your API key vulnerable to misuse.
5. **Conduct thorough code reviews**
   - Before pushing code to public repositories, always review it to ensure no sensitive information like API keys are exposed.
   - Use automated scanning tools that can flag potential leaks. You can check out Github's secret scanning tutorial for more.
   - When we detect an API key on the public internet or leaked inside an app in the app store, we will disable the API key immediately.
6. **Implement key rotation**
   - Periodically change your API keys by deleting old keys and creating new ones via the API key dashboard.

Understanding account takeovers

An account takeover occurs when someone gains unauthorized access to your account, potentially using our services and leaving you with the bill.

How to prevent account takeovers

1. **Use strong passwords or Google authentication**
   - For passwords, use a combination of upper and lower case letters, numbers, and special characters. We recommend using a password manager to generate and store passwords.
   - Update your password every few months.

2. **Enable multi-factor authentication (MFA)**
    - This adds an extra verification step, usually involving your phone.
    - Even if someone gets your password, they'd need the second factor to access your account.
    - Please note that enabling MFA *does not* cancel existing log-ins. To properly block any users accessing your account, you will first need to reset your password before enabling MFA.
3. **Be cautious with emails and links**
    - Be wary of emails that ask for your credentials or direct you to web pages that require you to input your account details.
    - Always double-check the email address and URL to ensure they're from a trusted source.

What to do if you suspect an issue

If you think your API key has been compromised or suspect unauthorized activity on your account, it's crucial to act quickly:

1. **Delete your API keys**
   You can delete your API keys via the API key dashboard. We also support tracking usage by API key. This makes it simple to view usage on a per feature, team, product, or project level, simply by having separate API keys for each.
2. **Contact us immediately**
   The sooner you report the issue, the faster we can help resolve it and minimize any potential damage. You can contact the OpenAI support team any time by opening a new chat in the bottom right corner of the Help Center.
3. **Review Account Activity**
   Check for any unfamiliar activity on your account, such as unexpected API usage. The detail you provide will help us restore your account.
4. **Log out of all devices.**
   You can log out of all of your active sessions across all devices by selecting this option. In ChatGPT, **Log out of all devices** can be found under Settings > Security and will disable your active ChatGPT sessions. On Platform, it can be found under Your Profile > Security and will disable your active Platform sessions. Please note that it may taken up to 30 minutes for other ChatGPT sessions to be logged out.

Conclusion

Security is a shared responsibility. While we take all necessary steps to protect your access, following these guidelines will further safeguard your account. If anyone uses your credentials without your permission, let us know ASAP. We'll do our best to help.

Related Articles

- How to delete your account
- Enabling Multi-Factor Authentication (MFA) with OpenAI
- How can I delete my OpenAI account in the ChatGPT Android app?
- OpenAI for Nonprofits
- OpenAI Account Sharing Policy

Did this answer your question?