Sharing your API key safely

A practical checklist for giving an API key to a faction tool, website or bot, and what to do if a key leaks.

Version 1.0. Published 23/11/2026, last reviewed 23/11/2026.

Introduction

Many faction tools and fan sites ask for an API key. Giving one is normal and, done carefully, safe: the API is read-only, so a key cannot move your money or items. But a key with a high access level exposes private information, such as your stats, money and activity, to whoever holds it. This guide is a checklist for sharing well.

How it works

What a key can and cannot do. A key lets its holder read data through the Torn API at that key's access level. It cannot log in as you, change your password, or take any action in the game. Your password is never needed by any tool, and Torn says tools must never ask for it.

Access levels limit what each key reveals: Public Only, Minimal, Limited and Full. Give each tool the lowest level it needs.

Control. You can hold up to 25 keys and delete any one at any time, which immediately stops that tool reading your data.

Who is responsible. Torn requires tool makers to keep keys and data confidential, and can ban those who misuse them. That protects you after the fact, not before.

Step by step

1. **Check who runs the tool.** Prefer tools your faction leadership or a well-known community member vouches for.
2. **Check the level it asks for.** A tool that only verifies identity should not need Full Access.
3. **Create a new key just for it.** Name it after the tool.
4. **Share it privately.** Enter it on the tool's own page or in a private message to the bot, never in a public channel.
5. **Read the tool's privacy notes.** Good tools say how they store keys (encrypted), what they read and how to delete your data.
6. **Delete keys you no longer use.**

If a key leaks: delete it in your settings straight away and create a new one for the tool. Deleting is instant and has no other effect on your account.

Examples

- Warden's Eye asks for keys only in private messages or on its own website, stores them encrypted, never shows them in Discord messages, and lets you delete your key at any time.
- A member pastes a Full Access key into faction chat by mistake. They delete it within a minute and create a fresh one; nothing else needs changing.

Advanced tips

- Separate keys per tool let you see which tool is making requests and cut off just that one.
- Ask tool makers how often they read your data; tools should request only what they need.

Common mistakes

- **Giving out your password.** No tool needs it, ever.
- **One Full Access key for everything.**
- **Posting a key in public channels or screenshots.**
- **Forgetting old keys** for tools you stopped using.

Sources

Torn wiki: API: https://wiki.torn.com/wiki/API, retrieved 2026-11-23

Torn API v2 reference (OpenAPI specification): https://www.torn.com/swagger.php, retrieved 2026-11-23

Related guides: Torn API fundamentals, Finding and joining a faction, Common mistakes