Warden's Eye Academy

The Torn API: all guides

What the API is, how keys and access levels work, rate limits, and how to share a key safely.

Contents

1. Sharing your API key safely (reviewed 23/11/2026)

2. Torn API fundamentals (reviewed 23/11/2026)

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

Torn API fundamentals

What the Torn API is, how keys and access levels work, selections, rate limits and error codes.

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

Introduction

The Torn API is Torn's official, read-only way for players and tools to fetch game data with an API key. Faction tools, browser extensions, stat trackers and the Academy's own price snapshots all use it. You do not need to understand it to play, but knowing how keys and access levels work helps you decide which tools to trust.

How it works

Read-only. The API only reads information. It cannot send money, attack, revive, trade or take any other action in the game. A tool that claims to do those things for you through the API is wrong, or is doing something else.

Keys. You create keys in your settings. Each key is 16 characters. You can hold up to 25 keys, each with its own access level, and delete any of them at any time. A key identifies you by itself, so a tool never needs your name, ID or password.

Access levels. Every key has one of four levels: Public Only, Minimal Access, Limited Access or Full Access. Higher levels expose more of your private data. The official API documentation lists exactly what each level can read.

Selections. A request asks for a section (for example user, faction or torn) and one or more selections within it. Torn's current API, version 2, is described in an OpenAPI specification that lists every path and the access level it needs.

Rate limits. Each user can make up to 100 requests per minute across all their keys. Too many requests get a key blocked briefly (error 5), and repeated invalid keys can get an IP address blocked (error 8).

Common errors:

Code	Meaning
2	Incorrect key
5	Too many requests
7	The data is private to someone else
10	The key owner is in Federal Jail
13	The key is disabled after 7 days of owner inactivity

The wiki lists codes 0 to 15. Torn's API documentation is the place to check for any newer codes.

Rules. Torn logs all requests. Tool makers must keep keys and data confidential, request as little data as needed, and must never ask for passwords. Torn can ban misbehaving applications,

keys and users.

Step by step

1. Open the API key section of your settings.
2. Create a new key for each tool, named after the tool.
3. Choose the lowest access level the tool says it needs.
4. Paste the key only into the tool's own setup page, never into a public chat.
5. Delete the key when you stop using the tool.

Examples

- A faction verification tool needs only a Public or Minimal key to confirm who you are.
- A tool that tracks your gym gains needs to read your battle stats, which requires a higher level; that is a reason to check who runs it.

Advanced tips

- One key per tool means you can cut off one tool without affecting the others.
- Keys of inactive players stop working after 7 days, so tools must handle error 13.

Common mistakes

- **Using one Full Access key everywhere.**
- **Thinking the API can perform actions.** It is read-only.
- **Sharing a key in a public channel,** where anyone can copy it.

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: Sharing your API key safely, Tracking chain contributions, Positions and permissions