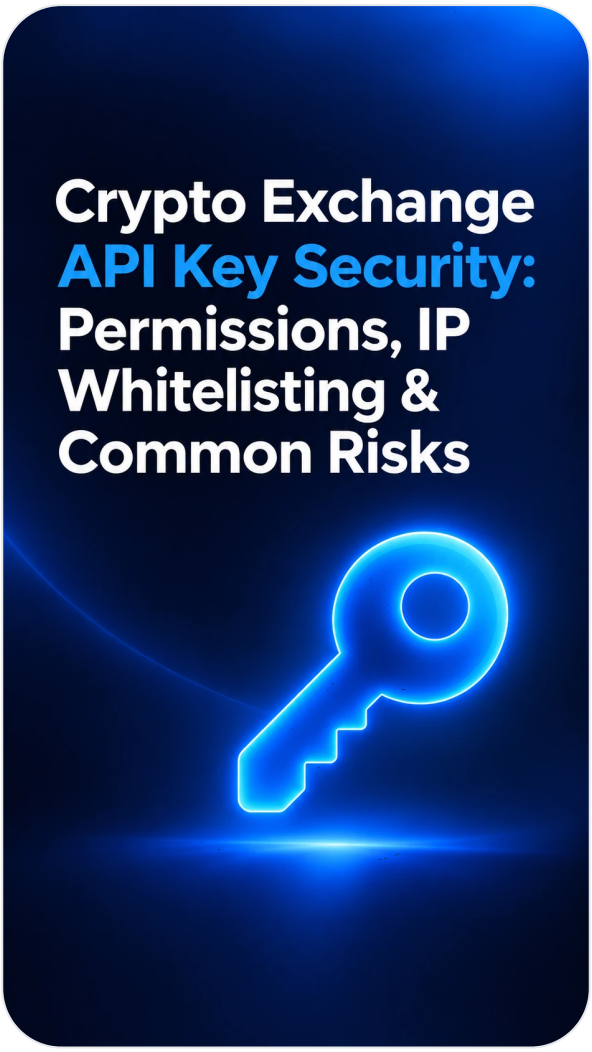

SECURITY & RECOVERY

Crypto Exchange API Key Security: Permissions, IP Whitelisting & Risks

By Matt Barnez

Written

Oct 18, 2026

API keys allow crypto exchange accounts to connect with trading bots, portfolio trackers, tax software, algorithmic trading systems, and other third-party services.

They can be extremely useful.

They can also create serious security risks if they are given more permissions than necessary, stored insecurely, or exposed to the wrong person.

A leaked API key does not always mean an attacker can withdraw your crypto. The damage depends on the permissions attached to the key and the security controls used by the exchange.

API permissions and security controls vary by exchange. Some platforms do not support API withdrawals at all, while others impose additional restrictions or require IP whitelisting for certain permissions.

Understanding how API keys work is therefore an important part of protecting your exchange account.

What Is a Crypto Exchange API Key?

An API key is a credential that allows another application to communicate with your crypto exchange account.

Instead of giving a trading bot or portfolio app your exchange username and password, you can create an API key and give that application limited access.

The exchange usually generates two important pieces of information:

- API Key
- API Secret

Some platforms may also use an additional passphrase.

Together, these credentials allow software to send authorized requests to your exchange account.

For example, a trading bot may use an API key to:

- check your account balance,
- read market data,
- place buy and sell orders,

- cancel open orders,
- manage positions.

The exact capabilities depend on the permissions you give the key.

Why API Keys Can Be Safer Than Sharing Your Login

API keys can improve security when they are configured correctly.

Instead of giving a third-party service full access to your account, you can limit exactly what it is allowed to do.

For example, a portfolio tracker may only need permission to read your balances.

It does not need permission to trade.

A trading bot may need permission to place orders.

It usually does not need permission to withdraw funds.

A useful rule is simple:

Give every API key only the minimum permissions required for its purpose.

The more permissions an API key has, the more damage someone could potentially cause if that key is compromised.

The Main Types of API Permissions

Most crypto exchanges divide API access into several permission levels.

The names vary between platforms, but the basic categories are usually similar.

Read-Only Permission

Read-only access allows an application to view account information without changing anything.

Depending on the exchange, this may include:

- account balances,
- transaction history,

- open orders,
- trade history,
- deposit records,
- withdrawal history,
- position information.

This is usually the lowest-risk type of API permission.

Portfolio tracking and tax applications often only require read access.

However, read-only does not mean completely harmless.

If an attacker obtains a read-only API key, they may be able to see sensitive information about your account, including your balances and trading activity.

That information could potentially be used for targeted phishing, social engineering, or account profiling.

Trading Permission

Trading permission allows an application to place and manage orders.

This may include:

- spot trading,
- futures trading,
- margin trading,
- order cancellation,
- position management.

Trading permission is commonly required for automated trading bots.

It creates significantly more risk than read-only access.

If an attacker gains control of a trading-enabled API key, they may be able to place unauthorized trades.

Even if withdrawals are disabled, they can still potentially cause financial losses.

For example, an attacker could:

- place unwanted buy or sell orders,
- open leveraged positions,
- close existing positions,
- trade repeatedly and generate losses,
- potentially use abusive trading strategies involving illiquid markets.

Disabling withdrawals therefore does not make a trading API key risk-free.

Withdrawal Permission

Withdrawal permission is usually the most sensitive API capability.

If the exchange supports API withdrawals and the key has withdrawal permission, an application may be able to transfer assets out of the account.

In most situations, third-party applications do not need this permission.

A trading bot needs to trade.

A portfolio tracker needs to read balances.

A tax application needs transaction history.

None of those normally need the ability to withdraw funds.

For this reason, withdrawal permission should generally remain disabled unless you have a specific and well-understood reason for enabling it.

If an exchange supports API withdrawals and a withdrawal-enabled API key is compromised, an attacker may be able to transfer assets directly out of the account.

That can turn an API leak into an immediate asset-loss event.

Why Withdrawal Permission Is Especially Dangerous

The risk is straightforward.

If withdrawals are disabled, an attacker may still be able to cause losses through unauthorized trading.

If withdrawals are enabled, they may also be able to move assets outside the exchange.

That creates a much higher level of exposure.

Some exchanges add extra protections such as:

- withdrawal address whitelists,
- API withdrawal limits,
- manual confirmations,
- security delays,
- IP restrictions,
- additional account verification.

These controls can reduce risk, but they should not be treated as a reason to enable withdrawal access unnecessarily.

The safest permission is the one you do not grant.

What Is IP Whitelisting?

IP whitelisting restricts an API key so that it only works from approved IP addresses.

This can significantly improve API security.

Imagine that your trading bot runs on a server with a fixed IP address.

You can configure the API key so that requests are accepted only from that server.

If someone steals the API key and tries to use it from another IP address, the exchange can reject the request.

This adds another layer of protection.

An attacker would need both:

- the API credentials,
- access to an approved IP address.

Why IP Whitelisting Matters

Without IP restrictions, someone who obtains your API credentials may be able to use them from another location.

With IP whitelisting enabled, the credentials become much less useful outside the approved environment.

IP restrictions are particularly valuable for:

- automated trading servers,
- private VPS systems,
- institutional trading infrastructure,
- self-hosted bots,
- backend applications.

If your exchange supports IP whitelisting and your application uses fixed IP addresses, enabling it is usually a strong security measure.

Some exchanges may also require IP whitelisting before enabling higher-risk permissions.

When IP Whitelisting Can Be Difficult

IP whitelisting is not always practical.

Some services use changing or dynamic IP addresses.

Cloud applications may send API requests from multiple servers.

Your home internet connection may also receive a new public IP address periodically.

In those situations, you need to understand how the third-party service handles API connectivity.

A legitimate trading platform should be able to explain whether it provides fixed IP addresses for exchange API connections.

If a service tells you to disable IP restrictions without clearly explaining why, that deserves additional scrutiny.

What Happens If an API Key Leaks?

The consequences depend on the permissions attached to the key.

A read-only leak may expose:

- balances,
- trade history,
- account activity,
- transaction information.

A trading-enabled leak may allow unauthorized:

- buy orders,
- sell orders,
- futures positions,
- margin trades,
- position closures.

A withdrawal-enabled leak may create the additional risk of assets being transferred out of the account, if the exchange supports API withdrawals and the required conditions are met.

The main question is not simply whether an API key has leaked.

The important question is:

What was that key allowed to do?

How API Keys Get Leaked

API keys can be exposed in many ways.

Common causes include:

- storing keys in plain-text files,
- uploading source code containing keys to public repositories,
- malware on a computer,
- phishing websites,

- fake trading bots,
- malicious browser extensions,
- compromised cloud servers,
- screenshots containing credentials,
- sending API secrets through messaging apps,
- poorly secured third-party services.

Developers also sometimes accidentally include API keys inside application code.

If that code is later uploaded publicly, automated scanners may discover the credentials quickly.

Treat the API Secret as a Sensitive Credential

Your API secret should be treated as highly sensitive.

Many exchanges display the API secret only once when the key is created.

After that, you may not be able to view it again.

This is intentional.

Do not store API credentials in:

- public notes,
- screenshots,
- unencrypted documents,
- shared spreadsheets,
- public code repositories.

If you believe an API secret has been exposed, do not wait to see whether someone uses it.

Revoke the key.

Trading Bots and API Security

Trading bots are one of the most common reasons users create exchange API keys.

A bot may need access to:

- balances,
- open orders,
- positions,
- trading functions.

This means users often need to enable trading permission.

Before connecting a bot, ask what permissions it actually requires.

If a trading bot requests withdrawal access, ask:

Why does this bot need to withdraw my assets?

For normal trading activity, it usually does not.

You should also check whether the bot:

- stores API keys locally or on its servers,
- encrypts stored credentials,
- supports IP whitelisting,
- has experienced previous security incidents,
- provides clear API security documentation.

A useful trading strategy does not automatically make the software itself trustworthy.

Portfolio Tracking Apps

Portfolio trackers usually require much less access.

Most only need read-only API permissions.

That may allow the application to see:

- balances,
- transactions,

- trading history,
- positions.

If a portfolio app asks for trading or withdrawal permissions, investigate why.

There should be a clear technical reason.

Otherwise, do not grant the additional access.

Tax Software and Accounting Tools

Crypto tax platforms may use API connections to import:

- trade history,
- deposits,
- withdrawals,
- transaction records.

In most cases, these applications should only need read access.

They should not need the ability to place trades or transfer assets.

Always compare the permissions requested by a service with what the service actually needs to do.

Use Separate API Keys for Different Services

Avoid using one powerful API key for every connected application.

Instead, create separate keys.

For example:

- one read-only key for portfolio tracking,
- one read-only key for tax software,
- one trading key for your bot.

This provides better control.

If one service is compromised, you can revoke its API key without affecting everything else.

Separate keys can also make it easier to identify which application is responsible for suspicious API activity.

Avoid Giving Every Key Maximum Permissions

Some users enable every available permission because it is easier.

That is a dangerous habit.

If an application only needs read access, give it read access.

If it needs trading access, enable trading but leave withdrawals disabled unless they are genuinely required.

This is known as the principle of least privilege.

Every service should receive only the permissions necessary to perform its function.

Nothing more.

API Keys and Subaccounts

Some exchanges allow users to create subaccounts.

Subaccounts can be useful for isolating trading activity.

Instead of connecting a trading bot to your main exchange account, you may be able to use a separate subaccount with a limited balance.

If the API key is compromised, the potential damage may then be limited to the assets held in that subaccount.

This does not eliminate security risk, but it can reduce the amount of capital exposed to a third-party integration.

Check API Activity Regularly

Many exchanges provide logs showing API activity.

These records may include:

- IP addresses,
- API requests,

- trading activity,
- creation dates,
- last-used dates.

Review these records periodically.

Look for:

- unknown IP addresses,
- unexpected trades,
- API activity when your bot was turned off,
- keys you no longer recognize,
- old API keys that are still active.

Security is not only about creating a safe API key.

It is also about monitoring it afterward.

Delete API Keys You No Longer Use

Old API keys create unnecessary security exposure.

If you stop using a trading bot, portfolio tracker, or other application, revoke its API key.

Do not leave unused keys active indefinitely.

Users sometimes create many API integrations over several years and forget about them.

Every active key is another credential that could potentially be compromised.

Periodically review the API management section of your exchange account and remove anything you no longer use.

Be Careful With Fake Trading Platforms

API keys are frequently targeted by scams.

A fake trading platform may promise:

- AI trading,
- automated arbitrage,
- guaranteed returns,
- copy trading,
- high-frequency trading,
- passive income.

It may then ask you to connect your exchange account using an API key.

Even if the platform tells you:

“Withdrawal permission is not required.”

that does not automatically make it safe.

A malicious platform with trading permissions may still be able to cause losses through unauthorized trades or other abusive trading strategies.

Do not connect your exchange account to a service simply because withdrawals are disabled.

Why Trading-Only API Access Can Still Cause Losses

Many users assume that disabling withdrawals completely protects their funds.

It does not.

An attacker with trading access may still be able to:

- buy or sell assets without permission,
- open risky leveraged positions,
- close positions at unfavorable times,
- create significant trading losses,
- potentially exploit thin or illiquid markets.

In some scenarios, abusive trading activity may also be designed to shift value between accounts or manipulate execution.

Exchanges use risk controls to detect suspicious behavior, but no security system eliminates every possibility.

Trading permission should therefore be treated as a sensitive capability.

API Keys and Two-Factor Authentication

Two-factor authentication protects many account actions.

However, API requests generally work differently from normal account logins.

Once an API key has been authorized, applications usually do not need to enter a new 2FA code for every API request or trade.

Security controls vary by exchange, but this is one reason API credentials must be protected carefully.

An attacker with valid API credentials may not need your account password or current 2FA code to perform actions that the API key is already authorized to perform.

2FA remains essential for protecting your exchange account, but it does not replace safe API configuration.

Should You Use Withdrawal Address Whitelisting?

If your exchange supports withdrawal address whitelisting, enabling it can provide additional protection.

This feature limits withdrawals to addresses you approved in advance.

Some exchanges also introduce waiting periods when a new withdrawal address is added.

This can make unauthorized transfers more difficult.

However, withdrawal address whitelisting should be considered an additional security layer.

It should not be used as justification for giving withdrawal permission to applications that do not need it.

What to Do If Your API Key Is Compromised

If you believe an API key has leaked, act quickly.

First, revoke or delete the affected API key directly from your exchange account.

Do not rely only on disconnecting the exchange from the third-party application. Removing a connection inside the third-party app may not invalidate the API key itself.

Then review:

- recent trades,
- open orders,
- withdrawal history,
- API activity,
- login history,
- other active API keys.

Cancel any unauthorized orders if possible.

If you believe your exchange account itself may also be compromised, change your password and review your two-factor authentication settings.

Contact the exchange immediately if you notice suspicious trading, account changes, or transfers.

You should also determine how the API key was exposed.

If the source was a compromised computer, trading bot, cloud server, browser extension, or third-party platform, creating a new API key without fixing the underlying problem could expose the new key as well.

Should You Create a New API Key After a Leak?

Yes.

Once an API secret may have been exposed, treat it as compromised.

Do not simply remove one permission and continue using the same credentials.

Revoke the old key and create a new one after addressing the cause of the leak.

API credentials are usually easy to replace.

Your funds are not.

Crypto Exchange API Security Checklist

Before connecting any application to your exchange account:

- Give the API key only the permissions the application actually needs.
- Keep withdrawal permission disabled unless there is a specific reason to enable it.
- Enable IP whitelisting when possible.
- Use separate API keys for separate services.
- Never share your API secret publicly.
- Do not store credentials in unencrypted files or public code repositories.
- Verify the reputation and security practices of third-party applications.
- Review API activity and suspicious trades regularly.
- Delete old or unused API keys.
- Revoke a key immediately if you suspect it has been exposed.
- Revoke compromised keys from the exchange itself, not only from the connected app.

Is It Safe to Use Crypto Exchange API Keys?

API keys themselves are not inherently unsafe.

They are a standard way for software applications to interact with crypto exchanges.

The risk depends on how they are configured and protected.

A read-only API key with IP restrictions and secure storage presents a very different risk profile from a key that allows unrestricted trading or withdrawals from any IP address.

The goal should be to reduce both permission and exposure.

Should You Give an API Key to a Trading Bot?

Only after understanding exactly what access the bot requires.

A legitimate trading bot may need trading permission.

It may also need read access to balances and positions.

It generally should not need withdrawal permission for ordinary trading.

Before connecting a bot, check its:

- security documentation,
- reputation,
- credential storage practices,
- IP restriction support,
- incident history.

If you cannot determine how the platform protects API credentials, think carefully before giving it access to your exchange account.

Can Someone Withdraw Crypto With a Read-Only API Key?

Normally, no.

A correctly configured read-only API key should not allow trading or withdrawals.

However, it may expose sensitive account information.

You should still revoke the key if it becomes compromised.

Can Someone Steal Crypto With Trading Permission but No Withdrawal Permission?

Potentially, an attacker can still cause serious financial losses.

They may not be able to directly transfer assets to an external wallet, but they could place unauthorized trades, open leveraged positions, or potentially use abusive trading strategies.

That is why trading permission should still be treated as sensitive.

Is IP Whitelisting Necessary?

It is not always required, but it can significantly improve security.

If your application operates from a fixed server or known IP address, whitelisting that IP can prevent stolen credentials from being used from an unapproved location.

For sensitive trading API keys, it is one of the most useful protections available.

Final Thoughts

API keys are powerful because they allow applications to interact directly with your crypto exchange account.

That same power creates risk.

The safest approach is simple:

Give each application the minimum access it needs.

A portfolio tracker should usually be read-only.

A trading bot may need trading access, but usually not withdrawal permission.

If IP whitelisting is available, use it when practical.

Keep API secrets private, remove unused keys, and regularly check your exchange account for unfamiliar API activity.

Most importantly, do not assume that disabling withdrawals makes an API connection completely safe.

An API key with trading permissions can still expose your account to serious losses if it falls into the wrong hands.

Treat API credentials like other high-value account credentials:

limit them, protect them, monitor them, and revoke them immediately when something looks wrong.