EXCHANGE

Crypto Exchange Account Hacked, Phished, or Locked? The Complete Recovery Guide

By Matt Barnez

Updated

May 24, 2026

Introduction

If your cryptocurrency exchange account has been hacked, phished, or unexpectedly locked, it can be both terrifying and confusing. This comprehensive guide explains why accounts may be compromised or frozen, including phishing attacks, SIM swaps, and compliance-related locks. It also helps you recognize the signs of a breach. It outlines the immediate steps you should take, such as securing your devices, changing your passwords, enabling two-factor authentication (2FA), and contacting support.

We provide detailed recovery instructions for major exchanges, including Binance, Coinbase, Kraken, Bitstamp, and Gemini. Additionally, the guide outlines how to collect evidence and logs, discusses expected response times, and includes templates for contacting support and law enforcement.

Moreover, the report covers best practices for prevention, including password managers, hardware 2FA, whitelisting, and alerts. We delve into business communication and public relations strategies for handling breaches, as well as legal and insurance considerations. It also highlights common mistakes to avoid.

Finally, the guide wraps up with a summary checklist and frequently asked questions (FAQ) to help you navigate through the recovery process effectively

Causes of Account Locks or Compromise

Exchange accounts can be frozen or compromised for various reasons. Common culprits include malicious hacks and social engineering attacks. Attackers often employ tactics such as phishing emails, fake websites or apps, and scam phone calls to deceive users into revealing their login credentials or seed phrases.

For instance, in a high-profile case in 2025, nearly $330 million in cryptocurrency was stolen not through hacking encryption, but solely via social engineering tactics, specifically, phishing victims into making unauthorized transfers. This highlights how human factors such as clicking on a malicious link, trusting a fraudulent app, or approving a spoofed transaction can often be the weakest link in security.

Additionally, techniques like SIM-swapping, which involves hijacking a user's phone number to bypass SMS two-factor authentication (2FA), and credential stuffing, where attackers use leaked passwords from other breaches, are well-known methods of compromise.

Malware on your device, including keyloggers, clipboard thieves, and malicious browser extensions, can also intercept passwords or seed phrases, further increasing the risk of account compromise.

Exchanges may lock accounts for reasons that are not related to hacking. For instance, Binance explains that suspicious logins or transactions, such as logins from a new country,y can trigger automatic locks to protect users' funds.

Accounts might also be frozen for compliance or security reasons, including interactions with known scammers, linking to illicit activities, missing KYC (Know Your Customer) or AML (Anti-Money Laundering) information, traveling to restricted countries, or responding to law enforcement requests. For example, Binance states that accounts can be locked if they are connected to sanctioned entities or if a user violates the platform's terms of use. Additionally, platform outages or maintenance can resemble a "locked account," so it's important to check the exchange's status page or social media for updates about downtime as part of your troubleshooting process.

In summary, don't assume the worst right away. While phishing and hacks are common, consider other benign causes like network glitches or compliance holds.

Signs Your Account May Be Compromised

Detecting a security breach early can help protect your funds. Be vigilant for unusual security alerts from your exchange, such as login notifications, password change confirmations, or notifications about updated phone numbers or email addresses that you did not authorize. These are important "red flags" that should not be ignored.

Additionally, if you experience login failures despite entering the correct password, especially if prompted for a password reset that shows an unknown phone number or email, this strongly indicates that an intruder may already have control of your account.

Carefully review your transaction and activity history. Any transfers, API keys, orders, or trades that you did not initiate are clear signs of compromise. Similarly, receiving an unusually high number of two-factor authentication (2FA) SMS code messages you did not request might mean attackers are attempting to log in to your other accounts (a practice known as credential stuffing) while overwhelming you with messages to obscure the legitimate code.

In summary, you should take immediate action if you notice any of the following major indicators: alerts about logins from unfamiliar locations or devices, unexpected emails about password or contact information changes, unauthorized transactions, or messages/codes you did not request. Even just one of these signs warrants a quick response. Do not assume it's a false alarm; act promptly if something seems off.

Immediate Response Steps (Containment & Assessment)

If you suspect that your account has been compromised or locked, act quickly but methodically:

1. Lock or Freeze Your Account (if available):

Some exchanges, like Coinbase, allow you to self-lock your account, which immediately logs you out of all devices. If there is a “Lock Account” or “Freeze Withdrawals” button, use it. This action will cut off the attacker’s access right away.

2. Change Your Password and Enable Two-Factor Authentication (2FA):

If you still have access to your account, change your exchange password to a strong, unique one (preferably generated by a password manager). Immediately enable or re-enable two-factor authentication (2FA) using an authenticator app or a hardware key. If the attacker has already changed your password, initiate a password reset through your registered email or phone. Once you regain access, change the login password and link a secure 2FA. Avoid using SMS for 2FA whenever possible; opt for authenticator apps or hardware keys to reduce the risk of SIM-swapping.

3. Secure Your Email:

Your email is often used as a recovery channel for exchanges, so assume it may also be compromised. Change your email password and enable 2FA immediately. Check your email's login history for any unknown access and revoke any unrecognized sessions. This step helps prevent attackers from using password-reset emails to take over your Exchange account.

4. Check Active Device Sessions and Log Out Others:

In your exchange account settings, look for active sessions or trusted devices. If you see any login sessions from unrecognized locations or devices, manually log them out. For example, exchanges like KuCoin list all active sessions; make sure to immediately remove any that you did not initiate. This ensures that no attacker remains logged in.

5. Stop any ongoing withdrawals.

If you notice funds being withdrawn, contact support immediately to freeze withdrawals. Check if your exchange allows for a withdrawal whitelist (as seen on Coinbase). If it does, enable it: with whitelisting activated, transfers can only go to pre-approved addresses and usually require two-factor authentication (2FA) to disable. This prevents attackers from draining your funds to new wallets. If a withdrawal is already in progress, notify support to block it.

6. Contact the exchange's support team:

Report the issue right away using only official channels (either the website or app chat). In your message, clearly state your account email/ID, the date and time of the incident, and request that all activity be paused or your account be frozen. Provide any details you may have, such as recent unusual logins or transactions. For instance, Binance advises: "Contact customer service… provide the required information (ID, proof of address, etc.) and follow their instructions." Kraken's advice is similar: submit a "suspicious activity" support form and provide as much detail as possible. Be patient but persistent, and keep records of all correspondence. Do not post your ticket publicly or respond to unsolicited support numbers or links—only use the exchange's official help desk.

7. Notify your banks or linked accounts:

If your account was connected to any bank or credit card, inform those institutions immediately to monitor for potential fraud.

8. Avoid further phishing attempts:

Attackers sometimes follow up with “customer support” scams that claim to help you. Remember, legitimate exchange support will never ask for your password or 2FA codes. Do not share one-time passwords (OTPs) or verification codes, and don’t click on new links unless you are certain they are genuine.

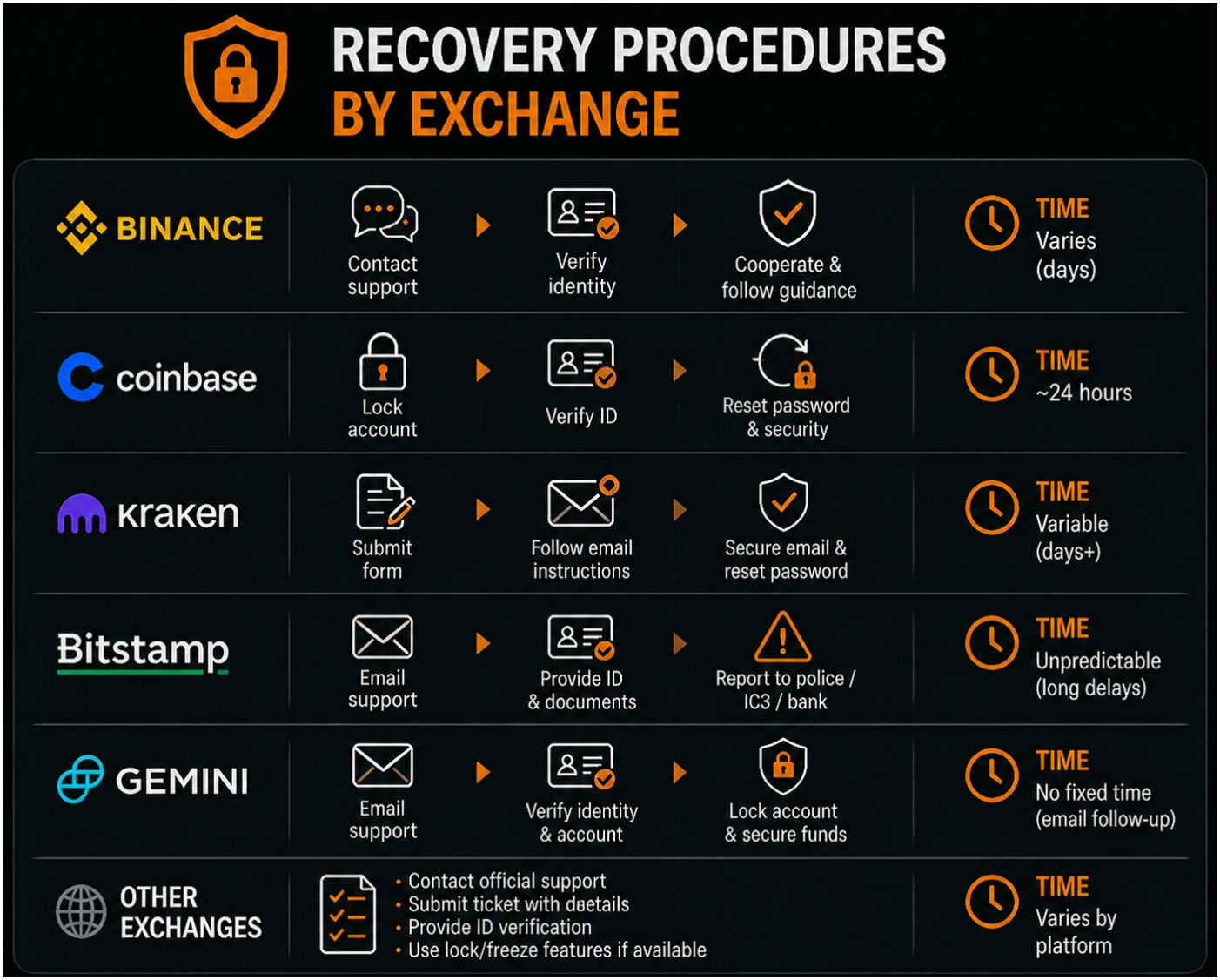
9. Collect evidence and logs:

As soon as possible, gather transaction IDs, timestamps, and any screenshots of fraudulent activity. Download or record your withdrawal and deposit history, and save any emails from the exchange regarding the breach. This documentation will be vital for investigations.

10. Report to authorities if applicable:

If a substantial amount has been stolen, consider filing a police report or reporting it to cybercrime units (e.g., the FBI’s Internet Crime Complaint Center in the U.S.). Providing evidence, such as transaction logs and wallet addresses, to law enforcement may assist in tracing or recovering funds.

Recovery Procedures by Exchange



Binance:

Binance does not offer an immediate self-lock feature, but you can get assistance from their support team. First, reach out via the official live chat or support form. Inform them that your account has been compromised or locked, and request urgent assistance. It is advisable to provide any requested verification (such as ID, proof of address, etc.) promptly and follow their instructions. For locked accounts, additional steps may be required. Binance warns that the resolution process can take time, especially if law enforcement or anti-money laundering checks are involved. In summary, contact Binance support, provide clear evidence of your identity, and fully cooperate with their guidance, which may include uploading identification and explaining recent transactions. Be sure to ask them to freeze all withdrawals in the meantime. Expected time: Varies (often days); the team will update you via email or chat.

Coinbase:

Coinbase offers a self-lock feature. If your account is compromised, you can immediately lock it using a special link on Coinbase, which will log you out of all devices. Then, attempt to log back in at Coinbase.com, where you will be prompted to verify your identity. To unlock a locked account, you must complete ID verification using a government ID or other documents. After your ID is verified, you will reset your password and complete any additional security steps. Coinbase notes that the verification process can take up to 24 hours. If you are not prompted for verification, contact Coinbase Support via their Help Center and mention “account compromised” to initiate your case. Expected time: Unlocking typically completes within approximately 24 hours once you submit your ID.

Kraken:

Kraken has a structured process for handling compromised accounts. Their support site directs you to fill out the Account Security & Sign-in Issues form, selecting “I’m concerned about suspicious activity.” Describe the situation in detail (including date, time, IP information, etc.). Kraken’s security team will follow up via email with instructions for securing your account and email. You will likely be asked to secure your email (by changing your password and enabling two-factor authentication) and reset your Kraken password as part of the recovery process. Kraken warns that this is a multistep process that may take time, and they ask for your patience and full cooperation. Expected time: Variable (can take multiple days or longer); Kraken emphasizes patience and following their emailed instructions precisely.

Bitstamp:

Bitstamp's public support resources regarding hacks are limited, so it's best to contact them directly. Immediately email support@bitstamp.net (or call their helpline) and state that your account was hacked or locked. Describe the situation and request a freeze on any activity. Be prepared to submit identity documents (such as ID and proof of address) to verify account ownership. It is also advisable to report the theft to the police, IC3, and your bank if funds were lost. Expected time: Unpredictable. Users report long delays. The best you can do is persist with support and provide all the requested information. If law enforcement gets involved, resolution could take weeks or months, and Bitstamp does not provide an official timeline.

Gemini:

Gemini instructs users to email Support through the official contact form, using the “Fraudulent Activity > My Account Is Compromised” category. In your email, include your full name, the email and phone number associated with your Gemini account, and explain the issue. If you must email from a different address, specify your Gemini account email. Gemini will respond with the next steps, typically involving identity verification and locking down withdrawals. Expected time: No fixed timeframe; Gemini support will follow up via email. Be prompt in your replies, and report any stolen funds immediately to the authorities.

Other Exchanges:

For any platforms not listed (e.g., Coinbase.com, KuCoin, Crypto.com, etc.), the general approach is similar: contact their official support, select any “account issue” or “security” category, and submit an urgent ticket with full details. Provide identity verification as required, and ask them to freeze your account. Additionally, try any built-in “lock” or “freeze” features they may offer.

Gathering Evidence and Logs

To support your case, it is essential to collect as much information as possible:

Transaction History:

Download or take screenshots of your exchange’s withdrawal and deposit history. Make note of the exact timestamps, transaction IDs, addresses, and amounts for any unauthorized transfers. This information is vital for investigators.

Login Logs:

Save records of all recent login activity, as many exchanges provide details about recent IP addresses or locations. Take screenshots of any unusual logins or multiple failed attempts.

Communications:

Keep copies of all emails or messages from the exchange regarding the hack or account lock. If you received any phishing emails or texts, make sure to preserve those as well.

Screenshots:

Capture the current status of your account, including balances, open orders, and any alerts.

Notes:

Write a timeline detailing what happened, including when you first noticed issues and the actions you took.

Experts recommend that sharing detailed evidence with both the exchange and law enforcement significantly aids the investigation. In one guide, victims were advised to “collect evidence related to your unauthorized transactions and share it with the exchange, local law enforcement, and the Internet Crime Complaint Center (IC3).”

When contacting customer support (e.g., Kraken), you will be required to answer questions thoroughly, so provide honest and detailed answers to expedite the process. The more logs and documentation you preserve from the beginning, the stronger your case will be for recovery or legal action.

Timelines & Expected Responses

Recovery timelines can vary significantly depending on the situation. User verification tasks, such as submitting identification, are generally quick, with Coinbase noting that ID checks can take up to 24 hours. However, if external investigations are required, the process may take longer. Binance explicitly warns that resolving account locks “may take some time” and advises users to be patient, especially if law enforcement or regulatory bodies are involved. Similarly, Kraken emphasizes the need for patience during their multi-step recovery process.

In practice, simple issues like forgotten passwords or device changes can usually be resolved within hours. However, an active hack or compromise may extend the recovery period to several days or even weeks.

Users should expect ongoing communication with customer support. Since exchanges often handle large volumes of inquiries, responses may not come immediately. For example, Bybit took approximately two weeks from detecting a breach to publicly disclosing it in February 2025, as they coordinated with law enforcement in the meantime. While Bybit's situation was internal, it illustrates that exchanges may need several days or more to fully assess and respond to a security incident.

In summary, make sure to change your credentials and contact customer support on the same day. Then, allow a few days for the exchange to verify and unlock your account. If needed, reach out to customer support every 48 hours for updates. If law enforcement is involved, they may conduct their own investigation on a different timeline. Be sure to keep track of all communications to monitor how long each step takes.

Sample Templates for Support & Law Enforcement

When contacting exchange support, it’s important to use a clear and factual tone. Your message should include essential details such as your full name, account email or username, and phone number if required. Clearly state that your account was compromised, mention the date and time, and note any unauthorized transactions. You should also explain that you have already taken initial steps like resetting your password and enabling two-factor authentication, and request that the exchange freeze all activity while guiding you through recovery. Attaching evidence such as screenshots and transaction IDs can help speed up the process.

If you need to contact law enforcement, keep your report concise and focused on facts. Explain that your cryptocurrency exchange account was accessed without authorization, describe what happened, and include key details such as the date, the exchange name, and the estimated value of the loss. Provide supporting evidence like transaction records, emails, and screenshots, and include your contact information for follow-up. Filing a report with local police or agencies like the FBI IC3 creates an official record, which may also be required by the exchange during any investigation or potential recovery process.

Prevention and Account Hardening

The best defense is prevention. Consider the following security measures to strengthen your exchange account:

Use Strong, Unique Passwords

Always create strong passwords that are at least 12 characters long and include a mix of character types. Never reuse passwords across different sites. A reputable password manager can help generate and securely store complex passwords. Remember to change your exchange password periodically.

Enable Two-Factor Authentication (2FA)

Always activate 2FA, ideally using an authenticator app or hardware key (e.g., YubiKey). This adds a crucial layer of security. Avoid relying solely on SMS for 2FA, as SIM swaps can intercept codes. Many exchanges, such as Coinbase and Gemini, support FIDO2 security keys for even stronger protection against phishing attacks.

Withdrawal Whitelists

If your exchange permits address whitelisting, use this feature. For instance, Coinbase's Address Book allows you to whitelist trusted withdrawal addresses. When whitelisting is enabled (usually requiring 2FA for changes), withdrawals can only be sent to your approved addresses, preventing stolen credentials from being used to send funds elsewhere.

Email Security

Secure the email account linked to your exchange with a unique password and 2FA. Many attacks target email accounts to reset Exchange passwords. If possible, use a separate email account exclusively for financial services and monitor it for security notifications.

Monitor Account Activity

Regularly check your account's login and transaction logs for any unusual activity. Some exchanges offer alerts or the option to log out sessions remotely. Early detection of suspicious activity allows for a quicker response.

Beware of Phishing

Be very cautious with emails, texts, or messages claiming to be from your exchange. Always verify the sender's address and domain. Do not click links in unsolicited messages; instead, visit the exchange's official site directly. Keep your web browser and email client updated to defend against malicious scripts. Binance specifically advises verifying the authenticity of emails and links before clicking.

Secure Your Devices

Install antivirus and anti-malware software on your computer and phone. Regularly update your operating system and applications. Avoid using jailbroken or rooted devices for financial transactions. Connect only through trusted networks, and consider using a VPN on public Wi-Fi.

Limit Exchange Permissions

If you use API keys or linked services, grant only the minimum required permissions (e.g., disable withdrawal permissions if not needed). Remove old or unused API keys.

Use a Password Manager

Utilize tools like KeePass, Bitwarden, or 1Password to securely store your crypto-related passwords and generate complex ones. This decreases the risk of forgetting passwords or writing them down insecurely.

Cold Storage

For large holdings, keep the majority of your funds in cold wallets (hardware wallets or paper wallets) and only a small amount on exchanges. While this does not directly address account compromise, it limits potential losses in case of an exchange hack.

Activate Device Trust and Alerts

Some exchanges allow you to mark “trusted devices” or notify you when a new device logs in. Enable these features if they are available.
By combining these precautions, you significantly increase the difficulty for attackers to breach your account. Even if one layer of security (such as your email) is compromised, additional layers (like hardware 2FA and whitelists) can help stop the attack in its tracks.

Communication and PR for Businesses

If your company or exchange experiences a breach or compromised accounts, clear communication is essential. Prepare an incident response plan in advance. When a breach occurs, quickly secure your systems and assemble a response team that includes IT, legal, and PR representatives.

Be transparent with your customers: create and publish an FAQ or status page that explains what happened, which data or accounts were affected, and how you are responding. For example, Bybit's public timeline shows they detected an attack on February 7, 2025, investigated it, and disclosed the breach on February 21. Such transparency—while withholding unconfirmed details—helps maintain trust.

Utilize multiple communication channels: email affected users, post updates on social media and your company blog, and ensure updates are provided regularly. Avoid jargon; explain technical issues in simple language. Highlight the steps customers should take for their safety (e.g., “Please reset your passwords”) and any remedies you will offer. If accounts or funds were compromised, work with legal counsel on notifications and compensation policies.

Internally, coordinate with law enforcement and cybersecurity partners. For instance, Bybit collaborated with authorities in March 2025 after its breach. Publicly assure users that you are working with experts to resolve the issue. Engage your legal and PR teams to comply with any disclosure laws applicable in your jurisdiction.

Above all, monitor public sentiment and counter misinformation. Promptly correct any rumors or scams that exploit the situation. Have prepared messaging ready to avoid causing panic (e.g., emphasize that user funds are safe or insured, if applicable). Good crisis communication can transform a PR nightmare into a demonstration of accountability and professionalism.

Legal and Insurance Considerations

It’s important to understand your legal obligations and protection options regarding cryptocurrency. In some jurisdictions, cryptocurrency accounts may be classified as personal property or securities, and the laws can vary significantly. If you experience a theft, make sure to report it to the relevant authorities, such as local police or cybercrime units, as well as any applicable consumer protection agencies.

If the value of the theft exceeds your insurance policy's threshold, your insurer may cover your losses, provided you have a policy in place. Keep in mind that many cryptocurrency policies require immediate reporting and thorough documentation of the incident.

Some large exchanges offer insurance for certain hacks or thefts (for example, FDIC-insured USD balances or coverage from third-party crypto insurers). However, this coverage typically applies only to platform-wide breaches and not to cases of individual account negligence.

Document everything related to the incident for any potential insurance claim: this includes police reports, communications with support teams, and any evidence you’ve gathered. Although legal recovery can be difficult if the attacker’s identity is unknown, law enforcement agencies may collaborate internationally to freeze stolen assets.

It's important to note that if your theft results from losing your own password, most exchanges will disclaim liability. However, if you can prove a flaw in the exchange's system, some companies may voluntarily reimburse affected users. Stay informed about any class actions or settlements; some lawyers monitor these cases and may recommend filing a claim against an exchange that failed to provide adequate protection.

Common Mistakes to Avoid

Victims often make mistakes that hinder their recovery. Here are some key errors to avoid:

1. Ignoring Early Warnings: Do not dismiss alerts about unfamiliar logins as one-time occurrences. Each warning could be your only clue before your funds disappear.

2. Using Unofficial Support Channels: Avoid calling phone numbers found through a Google search, as these are often scams. Always use the official support links provided by the platform.

3. Sharing 2FA/OTP Codes: Never disclose your SMS or authenticator codes to anyone. As Crypto.com warns, “Legitimate support will not ask for your OTP… never share those.”

4. Panicking and Moving Funds: Don’t rush to transfer funds to another wallet without a well-thought-out plan. This could lead to mistakes and worsen the situation. Instead, freeze withdrawals and carefully follow the support team’s instructions.

5. Neglecting Evidence: Failing to save logs or transaction records early on can limit your options for recourse. Start gathering evidence at the first sign of trouble.

6. Trusting "Recovery Services": Be cautious of any third party promising guaranteed recovery for a fee. These services are often scams. Stick to official channels and report issues to law enforcement.

By avoiding these pitfalls, staying calm, following official procedures, and securing your information, you can maximize your chances of recovery.

Conclusion

A hacked, phished, or locked crypto exchange account can feel overwhelming, but fast and organized action can make a major difference. The most important steps are to secure your email and devices, change passwords, enable strong two-factor authentication, freeze account activity if possible, and contact the exchange through official support channels. Collecting evidence early, such as transaction IDs, login records, screenshots, and emails, can also strengthen your recovery case with both the exchange and law enforcement.

At the same time, prevention is the best protection. Strong passwords, hardware-based 2FA, withdrawal whitelists, account alerts, and careful phishing awareness can greatly reduce the risk of future compromise. Crypto security depends on both the platform and the user. By staying alert, acting quickly, and using layered security, you can protect your assets and respond more effectively if something goes wrong.