P2P & DEFI

Crypto P2P Scams Explained: 10 Tricks Buyers & Sellers Use

By Matt Barnez

Written

Aug 30, 2026

Crypto P2P trading looks simple. A buyer wants crypto. A seller wants fiat. A P2P platform matches them, the buyer sends payment, and the seller releases the cryptocurrency.

But unlike a normal spot trade, part of the transaction happens between two people and often outside the exchange itself.

That creates opportunities for fraud.

A dishonest buyer may show a fake bank-transfer receipt and pressure the seller to release crypto that was never paid for. Another may make a real payment and later attempt to reverse it.

A dishonest seller may receive the buyer's money and then persuade the buyer to cancel the protected P2P order. Others try to move the conversation to Telegram or WhatsApp, where the platform's normal safeguards and evidence trail may no longer protect the user.

Modern P2P platforms use tools such as escrow, identity verification, risk monitoring, and formal dispute systems, but those protections still depend on users following the correct process. Binance's April 2026 P2P safety guidance specifically warns about fake payment confirmation, chargeback fraud, triangulation, phishing, third-party payments, and attempts to move users outside the platform.

This guide explains 10 P2P scam tactics, how they work from the victim's perspective, the warning signs to watch for, and what buyers and sellers should do instead.

Quick Answer: The 10 Common Crypto P2P Scams

#	Scam	Usually Targets
1	Fake payment receipt or SMS	Seller
2	Chargeback or payment reversal	Seller
3	Third-party or stolen-account payment	Seller
4	Triangle / payment-reuse scam	Seller
5	“Cancel after you paid” scam	Buyer
6	Off-platform / man-in-the-middle scam	Both
7	Fake support and phishing	Both
8	Extra payment or fake fee scam	Buyer
9	Appeal and cancellation manipulation	Both
10	Expired-order payment trap	Buyer

Bybit's March 2026 P2P security guidance separately identifies fake receipts, triangle attacks, impersonation, man-in-the-middle fraud, chargebacks, cancellation-after-payment scams,s and other social-engineering techniques among current P2P risks.

First: How Does Crypto P2P Trading Work?

In ordinary exchange trading, you might place an order such as:

Buy 1,000 USDT with another cryptocurrency.

The exchange's trading engine matches the order internally.

P2P trading is different.

You may instead choose an individual advertiser offering:

Sell 1,000 USDT for bank transfer

The process generally looks like this:

Buyer places P2P order

↓

Platform restricts or holds the seller's crypto for the transaction.on

↓

Buyer sends fiat using the agreed payment method.d

↓

Seller independently checks that payment arrived.

↓

Seller releases the crypto.

↓

Buyer receives the cryptocurrency.

Binance says its P2P marketplace uses an escrow mechanism to hold the seller's crypto during the transaction and also uses KYC and dispute-resolution features to reduce counterparty risk.

The dangerous moment is usually the gap between:

“Buyer says payment was made”

and

“Seller confirms the money actually arrived.”

Many P2P scams are designed to manipulate that gap.

The 10 Common Crypto P2P Scams

Scam 1: Fake Payment Receipt or Fake Bank Notification

This is one of the simplest P2P scams—and still one of the most important.

The buyer places an order for crypto.

Suppose the trade is:

$1,000 for 1,000 USDT.

Instead of actually transferring $1,000, the dishonest buyer sends the seller what appears to be proof of payment.

It may be:

A manipulated screenshot

A fake bank receipt

A forged transfer confirmation

A fake SMS

An edited banking-app image

The buyer then says:

“I already paid. Release the USDT.”

The seller sees something that looks convincing and releases the cryptocurrency.

But the money never actually arrived.

Binance explicitly warns that scammers can manipulate payment receipts and SMS notifications and advises sellers never to release crypto based solely on those materials.

Why This Scam Works

People often treat a bank screenshot as proof.

It is not.

A screenshot proves only that someone has presented you with an image.

It does not independently prove that your account received the money.

Modern editing tools make screenshots particularly weak evidence.

How Sellers Should Protect Themselves

Before releasing crypto:

Open your own banking or payment app.

Do not use the counterparty's screenshot.

Check the actual balance or transaction history.

Confirm that the money has arrived.

Verify the exact amount.

Do not assume a similar-looking incoming transaction is payment for the current order.

Verify the payer where the platform requires it.

The account holder should match the approved P2P counterparty under the platform's rules.

The fundamental rule is:

No money in your account = no crypto release.

Binance's current guidance says sellers should independently verify that payment is actually present before releasing crypto, regardless of any receipt or SMS shown by the buyer.

Scam 2: Chargeback or Payment Reversal

This scam is more sophisticated because the seller really does receive money initially.

A dishonest buyer sends payment.

The seller checks the account:

$1,000 received.

Everything appears legitimate.

The seller releases the crypto.

Later, however, the buyer disputes or attempts to reverse the fiat transaction.

Depending on the payment method and financial institution, the buyer may claim:

Unauthorized transaction

Mistaken payment

Fraudulent transfer

Account compromise

Another reason for reversal

If the payment is reversed after the cryptocurrency has already been released, the seller can potentially lose both:

the crypto

and

the fiat payment.

Binance currently identifies chargeback and reversal fraud as a major P2P risk and warns that some payment methods permit transactions to be challenged or reversed after the crypto has been released.

Why Chargebacks Are Dangerous in Crypto P2P

The two sides of the transaction behave differently.

The crypto transfer may become final once the P2P platform releases it.

But the fiat payment may operate under a financial system where reversal or dispute procedures exist.

That creates an asymmetry:

Crypto leaves permanently

while

Fiat may potentially be challenged later.

This is why sellers need to understand the payment method they accept—not simply whether the payment appears initially.

How Sellers Can Reduce the Risk

Use payment methods permitted by the platform and understand their reversal characteristics.

Avoid unusual arrangements that the counterparty claims are “basically the same” as the listed payment method.

Keep:

P2P order ID

Platform chat

Payment records

Counterparty details shown by the platform

Relevant transaction evidence

If a reversal occurs, raise an appeal promptly and follow the platform's dispute process.

Binance specifically recommends preserving transaction records and using the official appeal system when a payment reversal occurs.

Scam 3: Third-Party Payment

This is an extremely important warning sign.

Suppose your P2P buyer's verified name is:

John Smith

But the bank payment arrives from:

Michael Brown

The buyer may give a harmless-sounding explanation:

“That's my brother.”

“It's my business partner.”

“My friend paid for me.”

“It's our company account.”

Sometimes there may be an innocent explanation.

But accepting third-party payments can create substantial fraud risk and may violate the P2P platform's rules.

Binance warns sellers against accepting payments from third-party accounts because the actual account holder may later dispute the payment. Bybit also prohibits third-party payment in its P2P processes and warns users to compare payment-account names with verified P2P identities.

Why Would a Scammer Use Someone Else's Account?

One possibility is that the payment source does not actually belong to the buyer.

For example, the scammer may somehow have access to funds belonging to another person.

The seller sees real money arrive and releases the cryptocurrency.

Later, the actual account holder notices the transaction and disputes it.

The person who received the fiat—the P2P seller—may then be drawn into the dispute.

The Simple Rule

Compare:

P2P verified identity

with

Payment-account holder

If the platform requires them to match and they do not, do not casually accept explanations from the counterparty.

OKX currently states that buyers and sellers should cross-check the fund sender's name against the account holder information during P2P transactions.

Follow the platform's official procedure rather than improvising a workaround.

Scam 4: Triangle Scam

A triangle scam creates confusion between multiple trades or multiple people.

One current form described by major P2P platforms involves coordinated orders.

Imagine a seller has two open orders:

Order A

Buyer A owes:

$500

Order B

Buyer B owes:

$500

The scammers coordinate payments or reuse payment evidence in a way designed to make the seller believe both orders have been fully paid.

The seller becomes confused and releases crypto for more than the payment actually received.

Binance's April 2026 P2P guidance describes a triangulation scheme in which colluding buyers place simultaneous orders with the same seller, use partial payment and misleading claims, and try to cause the seller to release more crypto than was actually paid for.

Bybit also warns about triangle scams involving multiple orders and reused payment evidence.

Why High-Volume Sellers Are Vulnerable

Imagine processing:

30 P2P orders per day.

Several buyers may owe similar amounts.

If you look only at the total bank balance and see an incoming payment of $500, you might accidentally associate it with the wrong order.

That is exactly the type of confusion a triangulation attack attempts to exploit.

How to Protect Yourself

Verify every P2P order independently.

Match:

Order ID

Expected amount

Actual payment

Payer

Time

Never think:

“I received roughly the correct total amount today, so these orders must all be paid.”

Treat each order as its own transaction.

Binance recommends confirming the full and exact payment for each individual order before releasing crypto.

Scam 5: “Cancel the Order After You Paid”

This scam targets the buyer.

You create an order to buy crypto.

The platform places the seller's crypto under the normal P2P transaction controls.

You send the seller your payment.

Then the seller says:

“There's a technical problem.”

or:

“Please cancel and create a new order.”

or:

“Cancel first,t and I'll release manually.”

This should immediately concern you.

You have already sent the fiat.

Canceling the protected order may weaken or complicate the mechanism linking your payment to the cryptocurrency held for that particular transaction.

Bybit specifically identifies cancellation after payment scams and tells buyers not to cancel after they have already paid.

OKX gives the same basic warning:

Do not cancel a P2P order if you have already paid the seller.

What Should the Buyer Do Instead?

Once you have legitimately paid:

Mark the order according to the platform's normal payment process.

Keep the transaction active.

Keep communication inside the P2P chat.

If the seller refuses to release the crypto, open an appeal.

Do not cancel simply because the seller sounds convincing.

A Common Pressure Tactic

The seller may say:

“Cancel or your account will get restricted.”

or:

“I cannot release until you cancel.”

or:

“Support told me you need to cancel.”

Do not act based on the counterparty's description of platform rules.

Check the actual platform interface or official support.

Scam 6: Off-Platform and Man-in-the-Middle Scam

One of the biggest P2P warning signs is:

“Message me on WhatsApp.”

or:

“Let's finish the transaction on Telegram.”

The scammer may initially meet you through a legitimate exchange marketplace.

But once contact is established, they move the conversation away from the exchange.

Why?

Because the platform's normal protections may include:

Order records

Identity information

P2P chat history

Escrow mechanisms

Appeal evidence

Anti-fraud monitoring

Moving the conversation outside the platform can remove or weaken those protections.

How a Man-in-the-Middle Scam Can Work

A fraudster may position themselves between two legitimate people.

For example:

Person A believes they are dealing with the scammer.

Person B also believes they are dealing with the scammer.

The fraudster gives each person carefully selected payment or order instructions.

Eventually:

One victim sends fiat

while

another party releases crypto

and the scammer manipulates the transaction flow.

The exact forms vary.

The key warning sign is that the trade no longer follows one clear, verifiable P2P order between the matched buyer and seller.

Bybit's current P2P safety guide identifies man-in-the-middle scams involving external platforms such as Telegram, WhatsApp, and social media. KuCoin's current P2P guidance describes the same general pattern.

OKX Has Warned About This Exact Pattern

OKX reported in its May 2026 guidance that scammers were creating P2P advertisements and then pushing buyers toward WhatsApp, Telegram,m or other outside communication. Some then requested additional external payments and canceled the original P2P transaction.

The safe rule is straightforward:

One order. One platform. One in-platform conversation.

Do not allow the counterparty to transform a P2P order into a private transaction.

Scam 7: Fake P2P Support or Phishing

You have a problem with a P2P trade.

Suddenly someone contacts you:

“Binance Support here.”

“Bybit P2P Team.”

“Your transaction has been flagged.”

“Click this link to verify the payment.”

The person may know:

Which exchange you use

What cryptocurrency you trade

That you recently had a dispute

Details you posted publicly

That can make the message feel legitimate.

But scammers regularly impersonate exchange support.

Binance's 2026 P2P guidance warns that scammers may impersonate customer support through fake security messages designed to obtain login details or lure users to malicious websites.

Bybit likewise lists impersonation of its staff as a current P2P scam technique.

What Fake Support May Ask You to Do

Examples include:

“Release the crypto. The payment has been verified.”

“Your account will be frozen unless you act.”

“Send us your login code.”

“Click here to resolve your appeal.”

“Move your crypto to this verification wallet.”

These instructions should be treated as major red flags.

Never Let “Support” Override What You Can Verify Yourself

A support representative does not need to persuade you through a private social-media message to release funds.

Use:

The exchange's website/app

↓

Your actual P2P order

↓

Official appeal/support system

Do not click links from unexpected messages.

Protect Your Account Credentials

Never provide another person with:

Password

2FA code

Private key

Seed phrase

Remote access to your device

A P2P payment dispute does not require giving someone control of your crypto account.

Binance recommends navigating directly to the exchange website when receiving unexpected security messages instead of using links inside those messages.

Scam 8: Extra Payment or Fake Fee

You agree to a P2P trade.

The advertisement shows:

$1,000 total.

After the order begins, the seller says:

“You need to pay another $50 processing fee.”

or:

“My account is locked. Send an extra payment so I can release the USDT.”

or:

“There is a tax.”

or:

“Pay a verification deposit first.”

This changes the terms of the original transaction.

Binance's current P2P safety guidance lists sellers requesting additional fees not included in the original advertisement as a warning sign.

OKX has also warned about P2P scammers who move users outside the platform and request extra payments.

Why Small Extra Payments Are Effective

The first payment may already be large.

Suppose the buyer has sent:

$2,000.

The scammer then requests:

$50 more.

Psychologically, the buyer may think:

“I already sent $2,000. I'm not going to risk losing it over $50.”

That is exactly why additional-fee demands can be effective.

The buyer becomes focused on recovering the original payment and may continue sending more.

What Should You Do?

Do not send unlisted fees simply because the counterparty demands them.

Keep the trade within the original order.

If the seller changes the terms after payment:

Stop and use the platform's appeal system.

Do not solve one suspicious payment by making another suspicious payment.

Scam 9: Appeal or Cancellation Manipulation

Escrow and appeals protect P2P traders only when the user follows the correct process.

Scammers know this.

So rather than defeating escrow technically, they may try to persuade you to disable your own protection.

They might say:

“Accept the cancellation, and I'll refund you.”

“Click mutual agreement.”

“Close the appeal so I can transfer the crypto.”

“Support cannot help while the appeal is open.”

“Cancel this dispute, a nd we'll solve it privately.”

Do not treat these instructions as legitimate merely because they sound procedural.

Bybit Warns About “Mutual Agreement” Manipulation

Bybit's March 2026 P2P scam guide specifically warns that fraudsters may pressure users during an appeal to choose a Mutual Agreement option that can cancel the order and affect the disposition of the assets. It recommends independently confirming whether payment or refund has actually occurred rather than acting under pressure.

Platform interfaces differ, but the principle applies broadly:

Understand exactly what a cancellation, settlement, or appeal button does before clicking it.

Never Close a Dispute Based on a Promise

There is a big difference between:

“I will refund you after you cancel.”

and

“The refund is already visible in your account.”

Verify reality first.

Do not surrender platform protection in return for a promise that the counterparty will act afterward.

Scam 10: The Expired-Order Payment Trap

This one can catch buyers who are rushing.

A P2P order normally has a payment window.

For example:

Complete payment within the allowed time.

If the timer expires, the order may be canceled.

A dishonest seller may still say:

“Don't worry. Send the money anyway.”

or:

“The timer doesn't matter.”

or:

“I will send the crypto manually.”

The buyer pays after the protected P2P order has already expired.

Now the payment may no longer be tied to the original active escrow process.

OKX's May 2026 scam-prevention guidance explicitly warns users not to make payments after a P2P order has been canceled because of a timeout, noting that users can lose the protection of the platform's normal transaction process.

Why This Is Dangerous

Imagine the original order was:

$3,000 for USDT

with the seller's crypto associated with that active order.

The timer expires.

The P2P order is no longer active.

You then send $3,000 anyway because the seller promises:

“I'll send the USDT afterward.”

You have effectively transformed a protected P2P transaction into:

a direct payment to a stranger.

That is a very different risk profile.

What Should a Buyer Do?

If the order expires before payment:

Do not pay under the expired order.

Instead:

Follow the platform's current instructions.

Create a new valid order where appropriate.

Confirm that the new order is active.

Use only the payment details associated with that valid transaction.

If you already paid before the expiration but the interface creates a problem, use the official appeal process rather than making another payment.

Buyer Scams vs Seller Scams

Not every P2P fraud targets the same side.

Scams That Mainly Target Sellers

Scam	Seller's Main Risk
Fake payment proof	Releases crypto without receiving fiat
Chargeback	Receives fiat, releases crypto, then payment is reversed
Third-party payment	Payment may later be disputed
Triangle scam	Releases crypto against the wrong or insufficient payment

Scams That Mainly Target Buyers

Scam	Buyer's Main Risk
Cancel-after-payment	Buyer sends fiat but loses normal order protection
Extra fee	Buyer sends more than agreed
Expired-order trap	Buyer pays outside an active protected order

Scams That Target Both

Off-platform manipulation

Fake support

Phishing

Appeal manipulation

This is why there is no single P2P scam checklist that applies only to sellers.

Both sides have responsibilities.

The Most Important Rule for P2P Sellers

For a seller, the most important rule is:

Never release crypto because someone tells you they paid. Release only after you independently verify that the correct payment actually arrived.

That means:

Screenshot ≠ payment

SMS ≠ payment

“Payment Completed” button ≠ payment

Buyer promise ≠ payment

Your own payment account is the evidence that matters.

Binance explicitly identifies premature release based on receipts or notifications as a major avoidable P2P risk.

The Most Important Rule for P2P Buyers

For buyers:

Do not abandon the active P2P order after you have sent money.

If you paid the seller:

Do not casually cancel.

Do not move to Telegram.

Do not send an extra fee.

Do not close an appeal based on a promise.

Do not accept a replacement transaction outside the platform.

Use the platform's dispute process.

Bybit and OKX both specifically warn buyers not to cancel an order after payment has already been made.

What Does P2P Escrow Protect You From?

Escrow is one of the key security mechanisms in crypto P2P trading.

When a seller creates or accepts a P2P transaction, the platform can restrict the relevant cryptocurrency so that it cannot simply disappear while the buyer completes payment.

The buyer then pays the seller.

After payment is confirmed, the crypto is released.

This can help prevent a simple scam where:

Seller receives fiat → Seller disappears with both fiat and crypto.

Binance describes escrow as a central P2P protection because the seller's crypto is held during the transaction until the relevant release process occurs.

What Escrow Does NOT Protect You From

Escrow is not magic.

It cannot automatically know that:

A bank screenshot is fake.

A payment may later be reversed.

Someone is using a third-party bank account.

You are chatting with an impostor on Telegram.

You voluntarily canceled the protected order.

You paid after the order expired.

You shared your account credentials with a phishing site.

Security still depends on the buyer and seller following the platform's process.

How to Check a P2P Trader Before Trading

Before choosing an advertiser, review the information the platform provides.

Useful signals can include:

Number of Completed Trades

Someone with substantial trading history gives you more information to evaluate than a brand-new account.

Completion Rate

A very low completion rate can indicate unreliable behavior.

User Feedback

Read recent reviews where available.

Verified Merchant Status

Some platforms apply additional requirements to merchants.

Price

A price dramatically better than the rest of the market deserves extra scrutiny.

Binance's current P2P safety guidance recommends reviewing completion rate, total trades, and user feedback and treating unusually attractive prices with caution.

None of these factors guarantees that a trader is safe.

They are risk signals, not guarantees.

Red Flags When You Are Selling Crypto

Be cautious when a buyer:

Pressures you to release before the money arrives.

Sends only screenshots or SMS notifications as evidence.

Pays from a third-party account.

Sends a different amount from the order total.

Asks you to move to WhatsApp or Telegram.

Marks payment as completed but becomes unresponsive.

Asks for unusual personal information.

These are also among the warning behaviors identified in Binance's current P2P guidance.

Red Flags When You Are Buying Crypto

Be cautious when a seller:

Asks you to cancel after payment.

Changes payment instructions after the order begins.

Requests additional fees.

Wants to continue outside the platform.

Asks you to pay after the order has expired.

Promises to release crypto manually later.

Claims to be working with “support.”

Pressures you to close an appeal.

A legitimate P2P transaction should not require a complicated side arrangement.

Should You Communicate Outside the P2P Platform?

Preferably, no.

Keeping communication inside the platform gives investigators evidence if a dispute happens.

A message such as:

“Send another $200, and I will release the crypto”

is much easier for the platform to evaluate when it exists in the official order chat.

If that conversation takes place privately elsewhere, platform support may have far less evidence.

OKX explicitly advises users to preserve chat records and keep communications inside its P2P environment when dealing with suspected fraud.

What Should You Do If a P2P Trade Looks Suspicious?

Do not rush.

Follow this order.

1. Stop Before Releasing or Sending More

Pressure is a common scam tool.

A few extra minutes are usually safer than acting because someone says:

“Do it now.”

2. Keep the Order Active Where Appropriate

If you already paid, do not cancel simply because the seller requests it.

3. Keep Communication on the Platform

Do not switch to another app to “solve” the dispute.

4. Preserve Evidence

Save:

Order ID

In-platform messages

Payment confirmation

Bank transaction record

Counterparty information

Relevant screenshots

Dates and times

Do not edit or alter the evidence.

5. Open an Official Appeal

Use the dispute system attached to the actual P2P order.

Do not rely on a phone number or social-media account someone sends you.

Binance recommends stopping and gathering evidence when something appears wrong and opening a platform appeal rather than continuing under pressure.

What If You Already Released the Crypto?

Act quickly.

Save the transaction and order records.

Contact the P2P platform through official support.

Contact your bank/payment provider if the fiat side involves fraud.

Preserve all communications.

Report the counterparty through the platform.

Where appropriate, report suspected fraud to the relevant local authorities or cybercrime reporting service in your jurisdiction.

Do not pay someone who contacts you afterward promising guaranteed recovery.

Recovery fraud frequently targets people who have already lost money.

Do Not Fall for a Second Scam After the First One

This pattern is important.

You lose $5,000 in a P2P scam.

You post about it online.

Someone messages you:

“I'm a blockchain recovery expert.”

They claim:

“I found your crypto.”

Then they demand:

$500 recovery fee.

Do not assume that because the person knows details about your loss, they can recover anything.

Scammers actively target people who are already distressed.

The FBI similarly warns that fraud victims can be targeted again by fake recovery services claiming they can retrieve lost cryptocurrency in exchange for additional payments.

Is P2P Trading Automatically Unsafe?

No.

P2P trading itself is not a scam.

Major platforms have developed mechanisms intended to reduce risk, including:

Identity verification

Escrow-style transaction controls

Merchant screening

Risk monitoring

User histories

Appeals

Dispute resolution

Binance notes that these measures can substantially reduce counterparty risk.

But P2P still requires more active judgment than simply clicking Buy on a spot-market order.

The user participates directly in the settlement process.

That human interaction is where many scams occur.

Is a Verified P2P Merchant Guaranteed to Be Safe?

No.

Verification can reduce uncertainty but does not eliminate risk.

A verified or established merchant may provide:

More trade history

More reviews

Additional platform checks

But you should still independently verify every payment and follow the normal P2P process.

Never think:

“This trader has thousands of orders, so I don't need to check my bank account.”

Your security procedures should remain the same regardless of counterparty reputation.

Should Sellers Accept Third-Party Payments?

Generally, follow the platform's rules rather than accepting them casually.

Major P2P platforms warn about third-party payments because the person sending the money may not be the person buying the cryptocurrency.

Bybit states that third-party payments are prohibited under its P2P rules, while Binance warns that third-party account payments increase chargeback risk.

A buyer saying:

“Don't worry, it's my friend's account”

does not remove that risk.

Should Buyers Ever Cancel After Paying?

As a general P2P safety rule:

Do not cancel an order after payment unless the platform's official process clearly instructs you how to proceed and you have verified the relevant refund/resolution.

Bybit and OKX both explicitly caution buyers against canceling after payment.

If the seller will not release the crypto, use the appeal process.

P2P Safety Checklist for Sellers

Before releasing crypto, verify:

1. Did the money actually reach my account?

Not a screenshot.

1. Is the amount exact?

Match it to the specific order.

1. Does the payer comply with the platform's identity/payment rules?

Watch for third-party payments.

1. Is the order still active?

Do not improvise outside the order.

1. Is all communication inside the platform?

Preserve evidence.

1. Am I being pressured?

Pressure is a reason to slow down, not speed up.

1. Is there a dispute?

Use the appeal mechanism.

Only after those checks should the crypto be released.

P2P Safety Checklist for Buyers

Before and after sending fiat:

1. Check the seller's history and completion rate.
2. Confirm the payment details shown in the active order.
3. Send only the amount specified.
4. Do not make side payments or extra fees.
5. Do not move the conversation outside the platform.
6. Mark payment only after actually paying.

7. Never cancel casually after paying.
8. Do not pay after the order has expired.
9. Keep payment evidence.
10. Appeal if the seller refuses to release the crypto.

The P2P Rule That Prevents Many Scams

Think of every P2P transaction as one closed loop:

One verified counterparty

↓

One active P2P order

↓

One agreed payment

↓

One matching payment source

↓

One in-platform conversation

↓

One verified settlement

Scammers frequently try to break this loop.

They introduce:

Another bank account.

Another person.

Another messaging app.

Another payment.

Another order.

Another “support agent.”

Another explanation.

Complexity often benefits the scammer.

A legitimate trade should remain easy to connect from start to finish.

Brokerate Assessment

Crypto P2P fraud usually does not require hacking the exchange.

Instead, scammers attack the human settlement process.

They try to convince a seller that money arrived when it did not.

They make a payment that can later be challenged.

They introduce third parties so that the buyer's identity and payment source no longer match.

They create multiple orders to confuse sellers.

They persuade buyers to cancel after payment.

Or they move users outside the platform so the exchange's normal safeguards become less useful.

This is why Brokerate considers three controls especially important in P2P trading:

Verify the money independently.

Keep the transaction inside the active P2P order.

Never surrender escrow or appeal protection because the counterparty pressures you.

The platform can provide tools, but the buyer and seller still control critical moments in the transaction.

A seller who releases crypto based on a screenshot can bypass their own protection.

A buyer who sends money after an order expires can do the same.

In P2P trading, good security is therefore partly technical and partly procedural.

Final Verdict

Most crypto P2P scams exploit one of three things:

Fake information

“I paid.”

Reversible or suspicious payment

“The money arrived, but it later disappeared.”

Social engineering

“Cancel the order.”

“Message me on Telegram.”

“Send another payment.”

“Support told me to release.”

For sellers, the strongest protection is simple:

Never release crypto until you independently verify the exact payment in your own account.

For buyers:

Once you have paid, stay inside the active P2P order and use the platform's appeal process if the seller does not release the crypto.

For both sides:

Avoid third-party payments, off-platform communication, unexpected links, unofficial support,t and any attempt to make the transaction more complicated than the original order.

P2P security works best when the entire trade remains:

verifiable,   documented, and inside the platform's normal transaction process.