

Forum: [Hack Forums](#)

Thread: [Most Common Scam Tactics](#)

moonsh1n3 - March 25, 2026, 12:49 am

1) "Cloned Cards + PIN" Offers

How it's presented:

Vendors advertise cloned payment cards—often bundled with a PIN—as a simple shortcut to cash access. The pitch frames the transaction as low effort and low risk for the buyer.

Why it persuades victims:

It exploits a "too-easy" narrative: pay once -> withdraw cash. New or inexperienced users may underestimate real-world constraints (operational complexity, risk, and the fact that truly functional products would command much higher prices).

Why it's commonly a ripper product:

If a seller genuinely had a consistently "working" method that reliably produced cash-outs, selling it cheaply to strangers is economically irrational. The mismatch between claimed capability and bargain pricing is a strong indicator of fraud.

Typical red flags (research framing):

- Unusually low prices for "high success rate" claims

- "Guaranteed" outcomes, "no risk," or "works everywhere" language

- Refusal to use escrow; pressure to pay quickly

- Proof limited to screenshots/videos that are easy to stage

2) "Cheap Transfers" (PayPal, Cash App, Zelle, Western Union, etc.)

How it's presented:

Sellers claim they can initiate or facilitate transfers on demand and price them as a small fraction of the amount transferred, arguing they can do high volume and profit from scale.

Why it persuades victims:

The offer sounds like a "wholesale" model: many small margins add up. New buyers may accept that explanation without checking whether the pricing aligns with incentives.

Why it's commonly a scam:

If someone truly controlled a reliable way to move funds, they would typically seek a much larger share of the proceeds (or avoid retail buyers altogether). "10% of value" pricing is often a hallmark of a bait offer designed to maximize victim count.

Typical red flags:

- "Instant transfer" promises with no meaningful constraints

- Requirements to pay first, then "release" later

- Escalating add-on fees after payment ("verification," "unlock," "release fee")

Requests for sensitive personal data framed as “compliance”
Refusal to use escrow; pressure to pay quickly

3) Gift Card Code Fraud

How it's presented:

Rippers advertise discounted gift cards for major retailers (e.g., Amazon, Walmart, Home Depot). They promise immediate delivery of a code after crypto payment.

Why it persuades victims:

Gift cards are familiar, the value is easy to understand, and “digital delivery” feels plausible. Buyers may assume verification is simple, even though they can't safely validate the code pre-purchase.

Common ripper outcomes:

- No code delivered (block/ghost)

- A code delivered that's invalid, already redeemed, or region-locked

- “Partial delivery” followed by demands for more payment

Typical red flags:

- Large discounts with “guaranteed balance” claims

- No escrow, or “escrow disabled for digital goods”

- Reviews that are generic, repetitive, or suspiciously timed

4) “Non-VBV / Linkable Cards” Claims

How it's presented:

Sellers claim they can provide cards that bypass certain verification flows or are “linkable,” implying they're especially valuable and easy to monetize—yet they price them cheaply to suggest scale.

Why it persuades victims:

It leverages technical jargon and insider language to create authority. Newcomers may not know that genuinely rare, high-demand items are typically priced accordingly.

Why it's often fraudulent:

The key inconsistency is rarity vs. cheap price. When a vendor claims access to scarce “high-utility” items at bargain rates, it's frequently a reputation-laundering or churn-and-burn scam.

Typical red flags:

- Heavy use of jargon without verifiable detail

- “100% success” guarantees

- Claims of massive inventory for niche items

- Sales pressure and refusal of escrow/dispute mechanisms

Additional Scam Types to Include

Here are some other high-frequency darknet/deep web ripper tactics .

- “hacking services”

scammer will introduce himself as a professional Hack for facebook/ Instagram/email/company payroll” style offers—often just advance-fee fraud followed by ghosting or blackmail.

Counterfeit documents / “KYC bypass” packs

Fake IDs, bank statements, utility bills Commonly non-delivery, unusable templates, or recycled files.

Drop / reshipping scams

scammer provide a drop address” or “reshipper job” offers that either steal deposits or recruit victims into taking legal risk without payment.

Counterfeit Money

the scammer promises you to deliver a fake euro or dollar bills for a low prices which it will never arrives.

Fake escrow / “middleman” impersonation

Scammer poses as a trusted escrow service or a known community middleman using look-alike usernames/domains.

How to Avoid Getting scammed

Use trusted escrow—never a “seller-provided” escrow.

Only use an escrow system that is built into the platform you’re using or run by a well-known, independently trusted party. A common scam is when a “vendor” insists on using their escrow, a “partner escrow,” or a link they provide. In many cases, it’s simply the seller (or an accomplice) controlling the escrow and your funds.

Rule of thumb: if the escrow is introduced by the seller, treat it as untrusted until proven otherwise.

Be skeptical of “I know a guy” referrals and middlemen.

If someone claims they can “connect you” to a reliable seller or service, don’t treat that as proof of legitimacy. Scammers frequently operate multiple accounts and use one to “recommend” another to create fake credibility.

Safer approach: verify the seller independently through long-term reputation, consistent history, and community feedback that is hard to fake.

Do your research before you pay—not after.

Most victims only start investigating once they’ve already sent money. Instead, slow down and verify first. Look for:

A long, consistent history (not brand-new accounts)

Reviews that show specific details (not copy-paste praise)

Signs of reputation manipulation (sudden review spikes, repetitive language, “too perfect” ratings)

Watch for classic pressure tactics.

Scammers often push urgency: “limited stock,” “price goes up in 10 minutes,” “final slot today.” Legitimate sellers don’t need you to panic.

Rule: if you feel rushed, pause—urgency is often the scam.

Treat “too good to be true” pricing as a red flag.

Huge discounts on high-value outcomes are usually bait. When the promised value is high but

the price is extremely low, the most likely explanation is non-delivery.

Never pay outside agreed protections.

If a vendor asks you to move the deal off-platform, skip escrow “just this once,” treat it as a major warning sign. These are common ways to remove any dispute leverage.

Be cautious with “proof” (screenshots, videos, vouches).

Screenshots and short clips are easy to fake. “Vouches” can be bought, traded, or generated by alternate accounts.

Better signals: long-term consistency, verifiable track record, and feedback from reputable members over time.

the