Report | November 2026



The Gift Card

Fake Gift Card Rewards, Brand Impersonation & Survey-Based Monetization

Analysis by CTM360

CTM360®

CTM360®

INDUSTRY
E-Commerce

COUNTRY
All

REGION
Global

DATE
Nov, 2026

Threat Type
Reward-Based Scam

Threat Vector
Social Ads

Key Techniques
Fake Gift-Card Generation

Key Issue
Fake Reward Portal

OVERVIEW

CTM360 has identified **more than 1,000 incidents** associated with a recurring gift-card scam campaign that leverages fraudulent advertisements, celebrity-themed promotions, brand impersonation, and fake reward portals to lure users into deceptive verification and survey-based workflows. The campaign **exploits consumer trust** in well-known brands and retailers, including PlayStation, Google Play, Sephora, SHEIN, and Walmart, by falsely advertising gift cards and other rewards to attract user engagement.

The campaign redirects victims through a sequence of fraudulent pages designed to build credibility and encourage continued participation. This sequence typically involves a fake advertisement, brand impersonation, a fraudulent reward portal, gift-card selection, a simulated gift-card generation process, human verification, and a final stage involving surveys or deceptive offers. **No gift card was delivered in any flow tested by CTM360.** Instead, users were redirected to surveys, quizzes, application-installation offers, subscription pages, and SMS-based offers. These mechanisms appear designed to **generate affiliate revenue for the campaign operators**, indicating a reward-based social engineering campaign that exploits users through deceptive promises of gift-card rewards.



1 Fake Ad
The victim sees a sponsored social media ad or post promoting a free giveaway, gift card or exclusive reward.

2 Celebrity Claim
The ad uses a well-known celebrity or influencer's name, image or a fabricated endorsement to appear credible.

3 Brand Impersonation
Clicking through opens a page that copies a trusted brand's logo, colours and layout to make the offer look official.

4 Reward Portal
The victim is told they've been "selected" for a prize, often with countdown timers and fake winner comments to add urgency.

5 Fake Generation
A fake "generator" animation shows the reward being processed or unlocked, so the victim feels invested in finishing.

6 Verification
Before the reward is "released", the victim is asked to verify they are human or eligible to claim it.

7 Survey / Trap 10
Victims are pushed into surveys, app installs or paid subscriptions that capture PII and earn the scammers affiliate payouts. The reward never arrives.

Key Takeaway

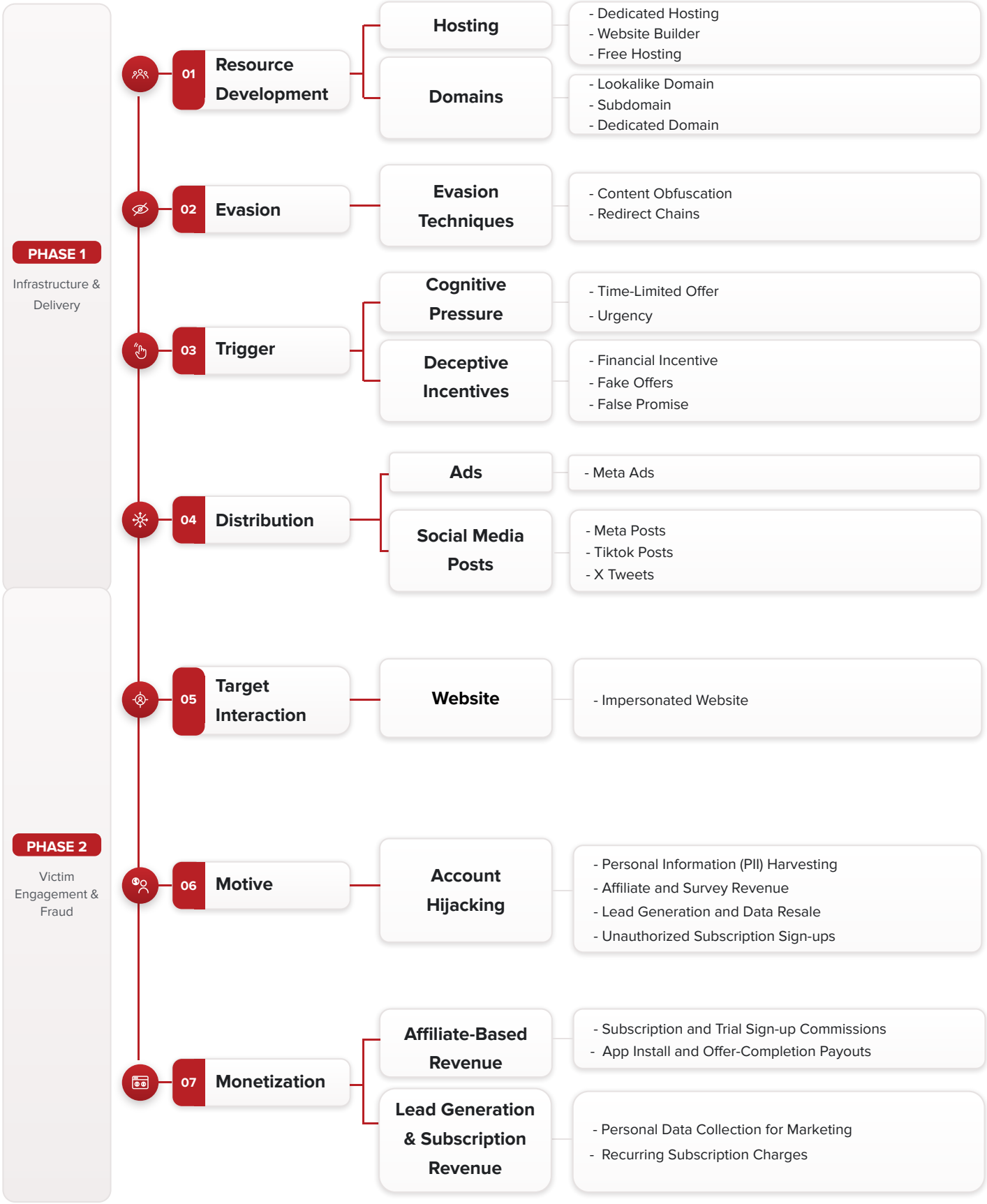
This campaign represents a scalable, reward-based social engineering and affiliate monetization operation that combines fraudulent advertisements, celebrity and influencer abuse, trusted-brand impersonation, and fake gift-card generation to funnel victims into survey and offer-based workflows. The promised gift card serves as **bait rather than a legitimate reward**, with the primary objective appearing to be driving users through multiple interactions to generate monetizable conversions. **Across more than 1,000 identified incidents**, the brand, celebrity, reward value, and domain vary, while the underlying workflow remains consistent. This operational consistency indicates a repeatable campaign model that can be deployed across different brands, audiences, and regions with minimal changes to its core infrastructure and processes.

Copyright @2026 **CTM360®**

FRAUD STAGES

CTM360 Fraud Navigator · The Gift Card Trap

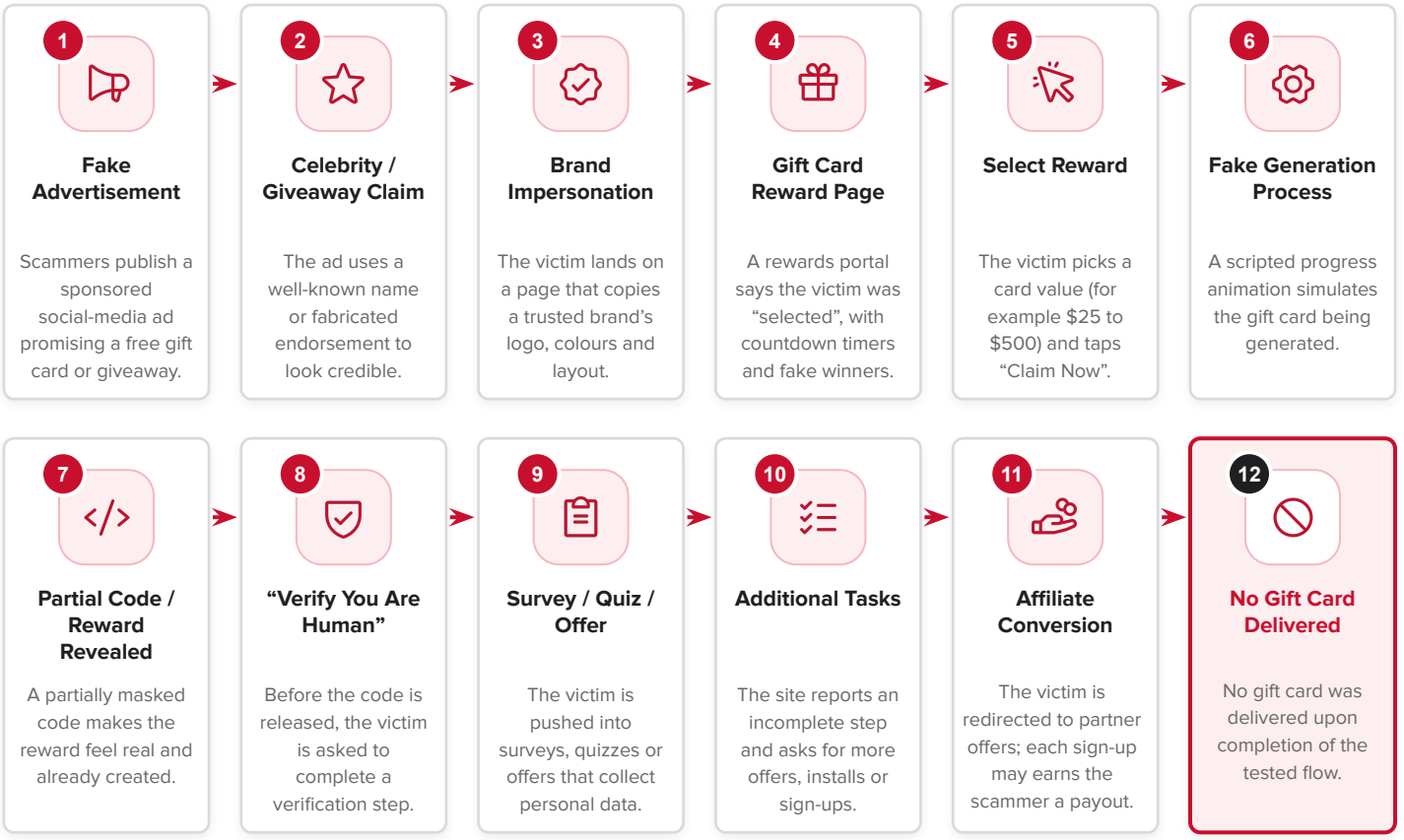
How the The GiftCardTrap campaign maps to each stage of the Fraud Navigator framework, across the infrastructure and victim-engagement phases.



Copyright @2026 **CTM360®**

Observed Attack Chain

The simplified flow below illustrates how a typical gift-card scam session unfolds, from the first advertisement to the point the reward fails to arrive.



VICTIM PSYCHOLOGICAL PROGRESSION

Curiosity → Trust → Expectation → Urgency → Action → Monetization

HOW THE VICTIM IS DECEIVED

- Celebrity and brand impersonation
- False promise of a free gift card
- Urgency: timers, "only 7 left"
- Artificial progress: fake generation
- Partial reward: masked code
- Pretext: "verify you are human"

WHERE THE CHAIN MONETIZES

- Survey completion
- Lead submissions
- Application installs
- Trial & subscription sign-ups
- SMS interactions
- Affiliate conversions

WHAT THE VICTIM LOSES

- Personal information exposed
- Subscription and mobile charges
- Unwanted apps and extensions
- Spam, phishing and scams
- Time spent with no reward

Copyright @2026 **CTM360®**

CTM360 OBSERVATIONS

Distribution Channel Breakdown

Social-media and sponsored advertisements serve as the primary victim-acquisition vector, with celebrity content and fake giveaway pages used to establish trust before the victim is routed through brand impersonation into the monetization stages.

01 Acquire	02 Build Trust	03 Engage	04 Monetize
Pull victims in at scale	Make the offer look legitimate	Keep the victim invested	Convert engagement into revenue
Social Media Ads Initial victim acquisition	**Celebrity Content** Trust and credibility	**Gift Card Generator** Maintain engagement	**Survey / Offer Pages** Affiliate conversion
Sponsored Ads Paid traffic generation	**Fake Giveaway Pages** Victim engagement	**Verification Page** Transition to monetization	**App / Extension Offers** Additional monetization
Viral Posts Organic-looking distribution	**Brand Impersonation** Establish legitimacy		**Subscription Pages** Recurring revenue

Key Takeaway

Because the brand, celebrity, reward value, and domain can all be swapped without rebuilding the operation, blocking one fraudulent site does little. The lasting defence is recognizing the pattern, a free reward, a countdown, and a verification step that asks for surveys or app installs. A genuine **gift-card redemption never requires them**.

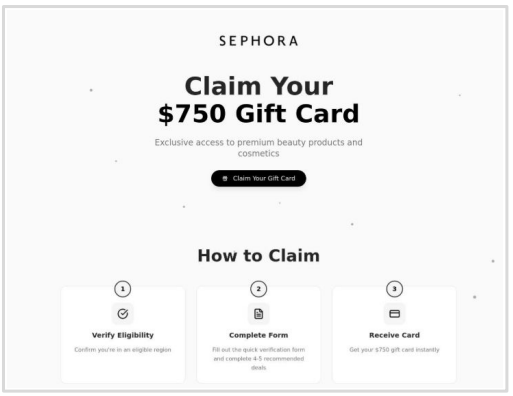
Copyright @2026 **CTM360®**

CTM360 OBSERVATIONS

Templates Observed

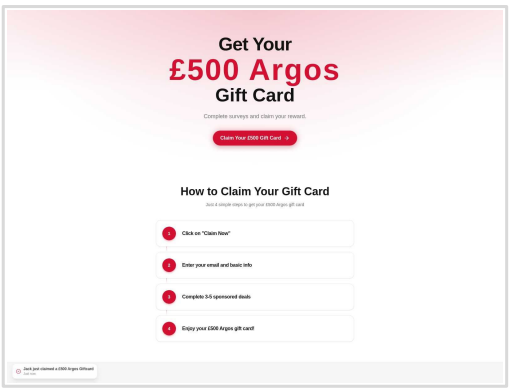
Across the **1,000 incidents** reviewed, CTM360 identified two main template categories: brand-specific templates imitating retailers such as Argos, Sephora, SHEIN, and Tesco, and generic templates featuring gift-card offers or celebrity giveaways, such as MrBeast.

BRAND-SPECIFIC TEMPLATES



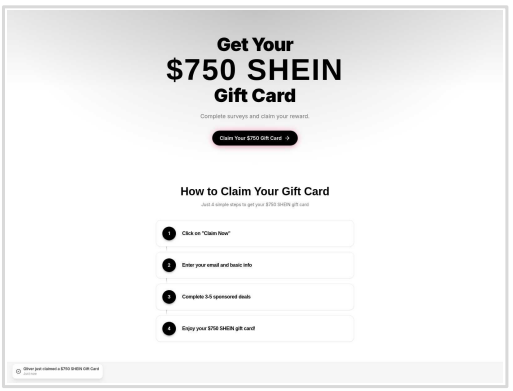
Sephora

Named-brand clone



Argos

Named-brand clone



SHEIN

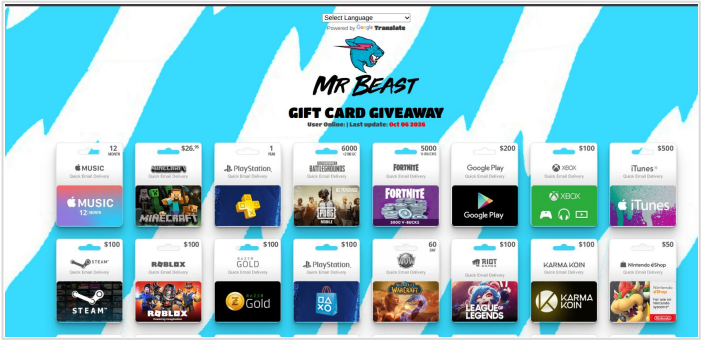
Named-brand clone



Tesco

Named-brand clone

GENERIC TEMPLATES



Celebrity Giveaway Grid (MrBeast)

No fixed brand -- swappable template



Gift Card Offer Portal

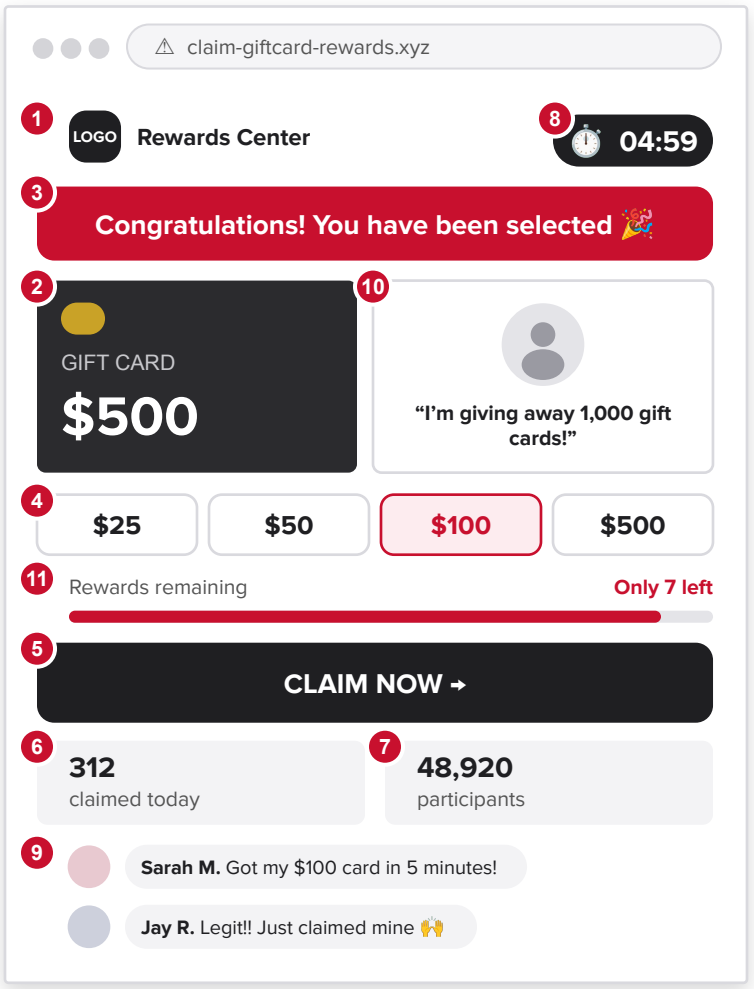
Generic template displaying multiple gift-card brands

Copyright @2026 **CTM360®**

Fake Reward Portal & Deceptive Incentives

After clicking the advertisement, the victim reaches a website designed to resemble a legitimate promotional or reward platform. It does not need to replicate the real brand's site, only to appear familiar enough that the victim does not immediately question its authenticity.

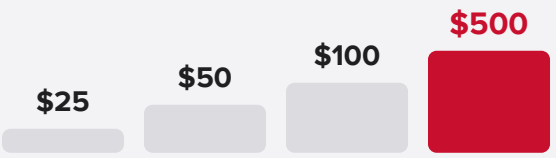
ANATOMY OF A FAKE REWARD PORTAL



TYPICAL PORTAL ELEMENTS

1. Brand logos
2. Gift-card graphics
3. Promotional banners
4. Reward amounts
5. "Claim Now" buttons
6. Giveaway counters
7. Fake participant numbers
8. Countdown timers
9. Testimonials & fake comments
10. Celebrity images
11. Reward availability indicators

SELECTABLE REWARD RANGE



DECEPTIVE MESSAGING OBSERVED

FALSE PROMISE
"Claim your free gift card."

URGENCY
"Limited-time reward available."

EXCLUSIVITY
"Congratulations! You have been selected."

SCARCITY
"Only a few rewards remaining."

TIME PRESSURE
"Claim before the timer expires."

VERIFICATION PRETEXT
"Complete verification to receive your gift."

Copyright @2026 **CTM360®**

The Fake Generation & Verification Trap

Once a reward is selected, the website simulates a legitimate back-end process to sustain the victim's engagement and belief that a real gift card already exists. It is only a scripted visual sequence, not a functioning generator.

1 Fake Generation
Scripted progress log

Generating your reward

Processing 96%

- Connecting...
- Generating...
- Checking inventory...
- Searching database...
- Validating code...
- Code generated
- Reward secured
- **Preparing your gift card**

A scripted sequence intended to create the appearance of a legitimate back-end process.

2 Partial Code Reveal
The hidden code is the bait

Your gift card is ready

GIFT CARD

YOUR CODE

XXXX-XXXX-**7F3A**-XXXX

"Reveal Full Code"

"Unlock Gift Card"

"Claim Reward"

A partially masked code makes the reward feel already generated. The hidden code becomes the bait for the final stage.

3 "Human Verification"
The pretext for the trap

Security check

Verification required

- "Verify you are human"
- "Complete verification to unlock"
- "One final step"
- "Confirm your reward"
- "Complete one quick survey"
- "Verify your eligibility"
- "Claim your reward in 10 seconds"

Redirect to survey / Trap 10 →

Key Takeaway

This is where the scam is likely monetized

WHAT THE VICTIM BELIEVES

They are completing a security requirement associated with the gift card.

WHAT ACTUALLY HAPPENS

The verification step redirects them into third-party, revenue-generating monetization activities.

Copyright @2026 **CTM360®**

Celebrity & Brand Impersonation

Recognizable celebrities, influencers, and trusted consumer brands are abused as credibility signals. The public figure or brand is not involved; the threat actor is exploiting their public image and reputation as a trust mechanism.

CELEBRITY / INFLUENCER ABUSE

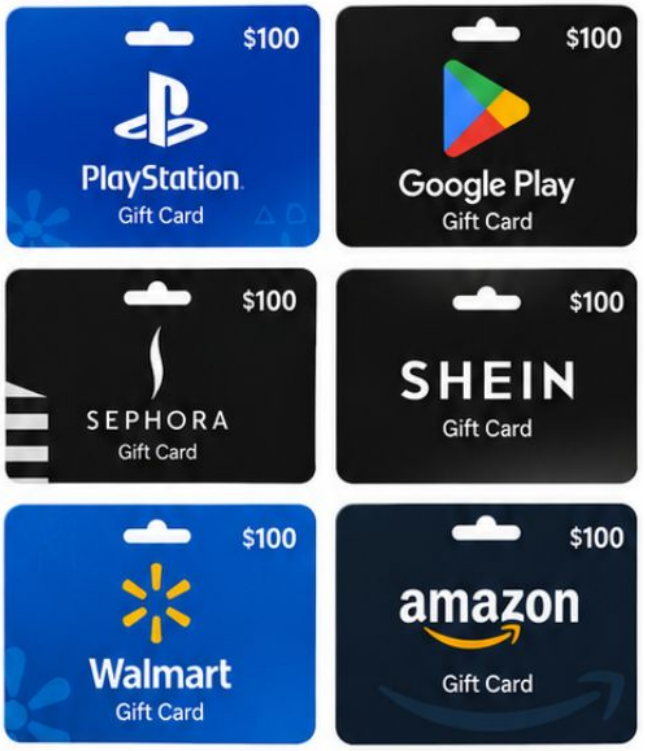


Source: X , @AbdoMjido6

- Celebrity photographs
- Fake quotes
- Fake giveaway announcements
- Fabricated interviews
- Fake social-media posts
- Edited promotional images
- Celebrity names in headlines
- Claims the celebrity is “giving away” gift cards

TRUSTED BRAND ABUSE

Observed gift-card themes impersonating well-known retailers:



The exact brand can change without significantly altering the underlying scam infrastructure, making the campaign highly scalable across audiences.

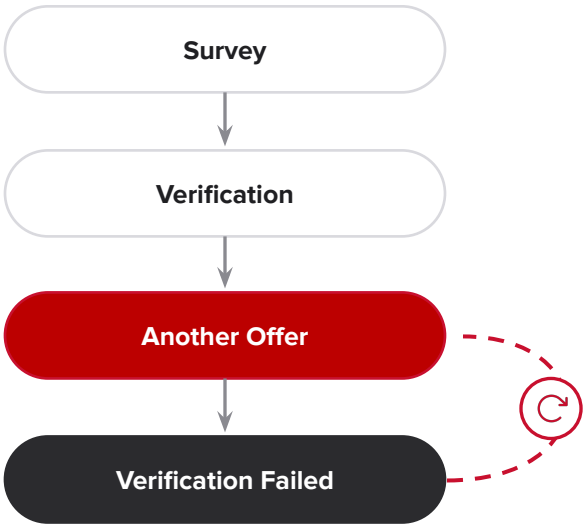
High-profile personalities such as MrBeast may be used because their public association with giveaways and large-scale promotions makes the fraudulent offer appear believable. **The celebrity association is not evidence that the individual or their organization is involved.**

Copyright @2026 **CTM360®**

The Endless Verification Loop

Completing the first task does not result in delivery of the promised reward. The website instead reports an incomplete step and redirects the victim to another offer, creating a repetitive cycle for as long as the victim continues.

THE VERIFICATION LOOP



After a failed check the victim is sent back to “Another Offer”, repeating.

MESSAGES OBSERVED

- “Verification incomplete.”
- “Offer not detected.”
- “Complete another offer.”
- “One more step required.”
- “Your reward is almost ready.”

WHAT THE VICTIM EXPERIENCES

At the end of the process, the promised gift card is generally not delivered.

No gift card
No reward was delivered in any observed session

STUCK IN THE FUNNEL

- Repeated redirects
- Additional surveys
- Continued promotional offers

INBOX & PHONE

- Spam messages
- Marketing communications
- Mobile charges

DEVICE & ACCOUNT

- Unwanted subscriptions
- Unwanted application installations
- Suspicious browser extensions

Key Takeaway

ACQUISITION MECHANISM
The fake gift card

→

MONETIZATION MECHANISM
The survey & offer wall

Revenue is generated from:

Survey completion | Lead submissions | Application installs | Trial & subscription signups | SMS interactions | Affiliate conversions

The attacker does not need to steal money directly from every victim.

Copyright @2026 **CTM360®**

Technical observation

This observed use case demonstrates a multi-stage gift card scam that uses a celebrity-themed lure to direct victims through two short surveys and a verification step before redirecting them to a third-party rewards site. Victims are prompted to provide an email address but receive no gift card, ultimately reaching a blank or non-functional page. The flow incorporates sign-up tracking to attribute user activity to the campaign's affiliate links, potentially enabling the operators to earn commissions from qualifying actions.

STAGE A · LURE SITE

amazonalix[.]lovable[.]app



Celebrity lure 08:40:03

"A gift for 5 million followers from yours truly, Alix Earle," shown with a $750 Amazon card.



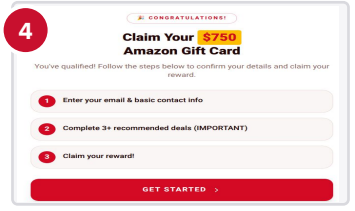
Qualifying survey 08:40:09

Question 1 of 2: "Do you live in the United States?" with an "Anonymous & Secure" badge.



Profile check 08:40:16

"Analyzing Profile" runs to 100%: checking availability, confirming eligibility, finalizing voucher.



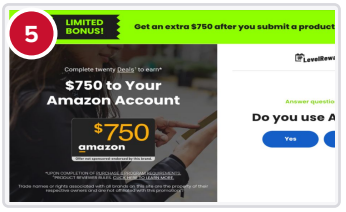
Claim screen 08:40:28

"Congratulations! You've qualified." Steps: enter email, complete 3+ deals, claim reward.

↪ **Victim is redirected to a third-party rewards site**

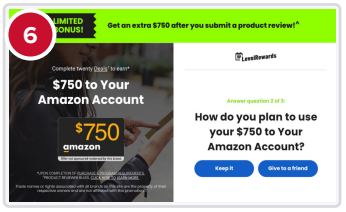
STAGE B · OFFER SITE

uplevelrewards[.]com



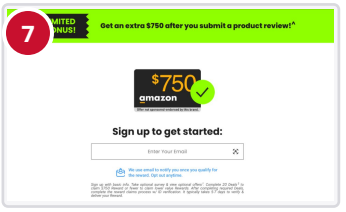
New site, new survey 08:40:38

A different domain asks "Do you use Amazon?" The reward now needs twenty Deals.



Engagement 08:40:51

Question 2 of 3: "How do you plan to use your $750?" Keep it, or give to a friend.



Email capture 08:41:01

"Sign up to get started." Fine print: complete 20 Deals, then 5–7 days to verify.



Dead end 08:41:33

A blank page showing only "AdFlow Active" and a tracking ID. No gift card was delivered during the observed session.

KEY OBSERVATIONS

Disposable hosting
The lure runs on a free app-builder subdomain, quick to create and easy to replace.

Moving goalposts
"3+ deals" on the lure becomes "twenty Deals" on the offer site, plus a 5–7 day verification wait.

Inconsistent Reward Requirements
The lure advertises reward eligibility after "3+ deals," whereas the destination site imposes a requirement to complete 20 deals, followed by a 5–7-day verification period.

Tracked hand-off
The lure redirects victims through affiliate tracking URLs to registration and offer pages. Embedded parameters support traffic attribution.

INDICATORS

LURE DOMAIN	**amazonalix[.]lovable[.]app**
OFFER DOMAIN	**uplevelrewards[.]com**
LANDING PARAMS	**lp=reviewerbonus750 · reward=amazon750rvw · isPrePop=true**
END PAGE	**default.aspx** "AdFlow Active"
ABUSED IDENTITY	Amazon (Brand), Alix Earle (Influencer)
SESSION LENGTH	≈ 90 seconds, 8 screens

Copyright @2026 **CTM360®**

Technical observation

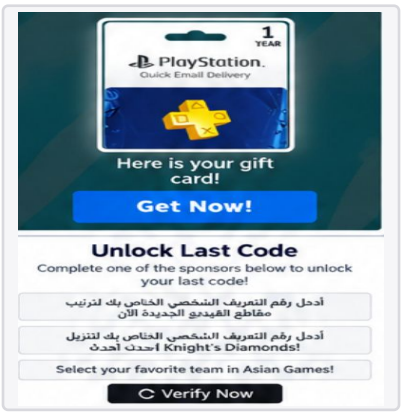
This observed use case illustrates how a gift card scam uses MrBeast's celebrity branding to lure victims through a fake "human verification" step to a third-party reward or subscription page. Victims are prompted to provide personal information, demonstrating the Trap 10 technique, while a threat actor tracking token links their registration to the scam campaign.

1 STAGE A · LURE
Celebrity giveaway lure



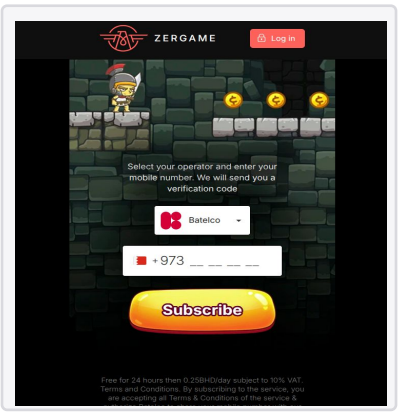
"MrBeast Gift Card Giveaway" page displays multiple gift-card rewards and a claim flow.

2 STAGE B · VERIFICATION
"Last Code" verification



The selected PlayStation gift card is displayed; however, the page states that the final redemption code remains locked until the user completes at least one sponsor offer. The sponsor offers were presented in Arabic, consistent with the test location.

3 STAGE C · CAPTURE
Mobile subscription capture



The offer flow redirects users to a localized subscription page requesting a mobile number and promoting recurring carrier billing.

TRAP 10

PHONE-NUMBER CAPTURE

Phone-number capture

The final step redirects users to a paid mobile subscription offer. The victim is pushed from a prize claim to sponsor offers and then to phone-number submission for carrier billing.

Carrier billing | PIN-confirmed sign-up | Daily auto-renewal

KEY OBSERVATIONS

Celebrity impersonation
The lure borrows a well-known creator's branding and giveaway format to establish trust.

Prize-to-verification pivot
The promised gift card is replaced by a requirement to complete a sponsor offer.

Offer-wall monetization
Localized sponsor offers guide victims into the subscription funnel, with language varying by region.

Localized carrier targeting
The final page adapts to the victim's region, displaying relevant dialing codes and recurring subscription charges.

INDICATORS

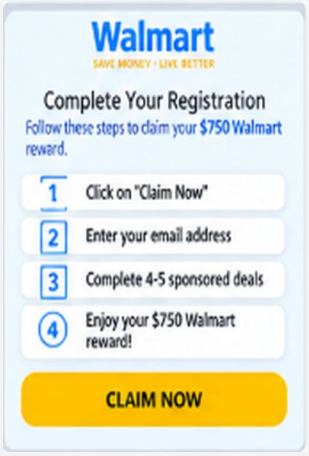
LURE SITE	celebrity-themed giveaway / gift-card claim page
VERIFICATION	fake "Unlock Last Code" / complete-one-offer gate
END SITE	The final page displayed to the victim, with content tailored to their location.
DATA CAPTURED	Requests a mobile number formatted according to the victim's country.

Copyright @2026 **CTM360®**

Technical observation

Technique 1: Reward Registration and Affiliate Tracking

STEP 1 Reward Registration Lure



Registration page (gift-card / offer page)

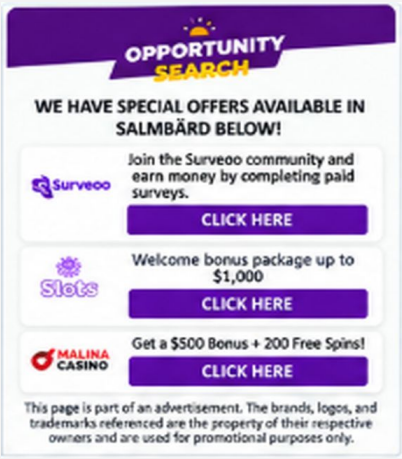


HTML/DOM evidence showing affiliate tracking link

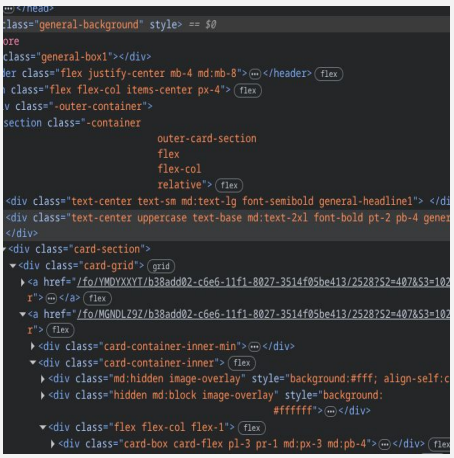
The lure page redirects victims through an affiliate tracking URL (e.g., https://trksy.org/aff_c?offer_id=1911&aff_id=19****) to a registration or offer page. The destination prompts users to enter their email address and complete four to five sponsored deals. The URL structure indicates the use of affiliate tracking to associate referral traffic with specific campaign parameters.

Observed redirect URL: https://trksy.org/aff_c?offer_id=1911&aff_id=19****

STEP 2 Sponsored Offer Selection & Attribution



Sponsored offer page presented to the victim



Affiliate link in page source / inspector

Selecting a sponsored offer or survey redirects the victim through a URL containing tracking parameters. These parameters may be used to attribute referral traffic and subsequent qualifying actions to an affiliate account. Although the observed redirect structure is consistent with an affiliate-based monetization workflow, it does not independently establish that the action was completed successfully or that a commission was generated or paid.

Observed redirect path : /fo/FFGEYELF/837a0a30-c6d6-11f1-9767-b17d4274b910/2528?S2=407&S3=102854dbb35638f0302a2c1c243fe5

Victim redirected to reward registration page → Victim submits email / registration details → Victim views or selects sponsored offer → Potential qualifying action → Potential affiliate attribution or commission (unconfirmed)

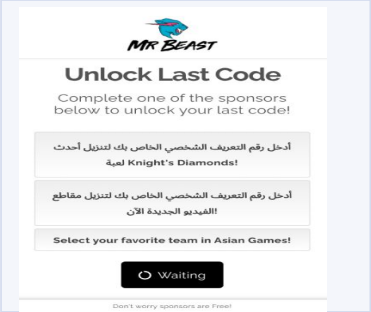
Copyright @2026 **CTM360®**

Technical observation

Technique 2: Affiliate-Based Subscription Redirection

1 STAGE A · VERIFICATION

"Last Code" verification

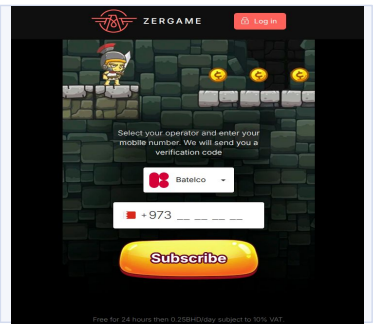


Locked code / sponsor offers

The selected PlayStation gift card is displayed; however, the page states that the final redemption code remains locked until the user completes at least one sponsor offer. The sponsor offers were presented in Arabic, consistent with the test location.

2 STAGE B · CAPTURE

Mobile subscription capture



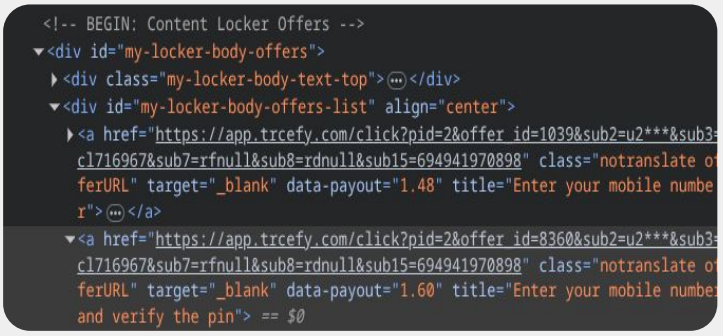
Subscription page

The offer flow redirects users to a localized subscription page requesting a mobile number and promoting recurring carrier billing.

Phone-number capture

The final stage redirects victims from a gift-card claim flow to a localized subscription page that requests a mobile number and presents a carrier-billing offer. This redirects the user from the promised reward to a potential paid subscription. The presence of subscription terms and phone-number fields does not, by itself, confirm that a subscription was activated or that recurring charges were applied.

- Carrier billing
- PIN-confirmed sign-up
- Daily auto-renewal



HTML/DOM details with affiliate tracking link

Observed redirect URL:

https://app.trcefy.com/click?pid=2&offer_id=8368&sub2=u22****&sub3=c1716967&sub7=rfnull&sub8=rdnull&sub15=494941970898

The offer link contains affiliate tracking parameters, including sub2=u22**** (partially masked in the report). This value represents the affiliate ID assigned to the threat actor by the affiliate network. When a victim completes the subscription (mobile number submission and PIN/OTP verification), the registration is attributed to this affiliate ID, allowing the threat actor to receive a commission from the affiliate program. The victim is redirected to a carrier-billed subscription service.

Gift-card lure → Affiliate tracking link with (sub 2) parameters → Mobile number requested → PIN/OTP subscription → Potential affiliate commission

Copyright @2026 **CTM360®**

Victim Impact

The impact of this campaign extends well beyond simply not receiving the promised gift card. Potential consequences accumulate across each stage the victim is pushed through.

IMPACT BUILDS AT EVERY STAGE



Personal Information Exposure — DATA

Email addresses, phone numbers, names, and other information may be submitted to third-party forms.

Subscription Charges — MONEY

Victims may unknowingly enroll in recurring services or free trials.

Mobile Billing — MONEY

SMS-based offers may result in unexpected charges.

Unwanted Applications — DEVICE

Victims may install applications to satisfy the fake verification requirement.

Browser Risk — DEVICE

Users may be encouraged to install extensions that affect browsing activity or request extensive permissions.

Increased Spam — DATA

Submitted contact information can be reused for additional marketing, phishing, and scam campaigns.

Lost Time — TIME

Victims may complete multiple tasks without ever receiving the promised reward.

RED FLAG

A legitimate gift-card redemption process should never require completing unrelated surveys, installing third-party software, or navigating arbitrary offer walls before the reward is delivered.

Copyright @2026 **CTM360®**

Motive & Monetization

The monetization model differs from traditional credential-stealing phishing. Rather than requiring direct theft from every victim, the campaign attempts to generate revenue through high-volume user acquisition and conversion.

TRADITIONAL PHISHING

Direct theft from each victim

Value depends on stealing credentials or money from every person who is caught.

VS

THIS CAMPAIGN

Volume and conversion

Value comes from moving many victims through the funnel until enough of them convert.

THE OPERATIONAL MODEL



SWAPPED WITHOUT REBUILDING

- Targeted brand
- Celebrity
- Reward value
- Advertisement
- Landing domain

This model allows threat actors to operate at scale while continuously changing elements.

SIX TECHNIQUES BEHIND GIFT CARD SCAMS

Advertising abuse	Brand impersonation	Celebrity exploitation
Deceptive incentives	Fake gift-card generation	Survey-based monetization

Key Takeaway

The Gift Card scam campaign represents a scalable, reward-based fraud model. The attack does not rely solely on convincing a victim that a fraudulent website is legitimate. It gradually builds commitment through multiple stages before **the final verification step, which is the actual trap.**

Copyright @2026 **CTM360®**

ABOUT US

CTM360 provides a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and fully managed unlimited takedowns), security ratings, third party risk management, email intelligence (dmarc) and cyber threat intelligence.

CONTACT US:

+973 77 360 360

info@ctm360.com

www.ctm360.com

21st Floor, East Tower Bahrain Financial Harbour, Kingdom of Bahrain

Disclaimer

The information contained in this document is meant to provide general guidance and brief information to the intended recipient pertaining to the incident and recommended action. Therefore, this information is provided "as is" without warranties of any kind, express or implied, including accuracy, timeliness, and completeness. Consequently, under NO condition shall CTM360®, its related partners, directors, principals, agents, or employees be liable for any direct, indirect, accidental, special, exemplary, punitive, consequential, or other damages or claims whatsoever including, but not limited to loss of data, loss in profits/business, network disruption...etc., arising out of or in connection with this advisory.

RECOGNIZED IN THE
2026 Gartner ® Magic Quadrant ™
For Cyber Threat Intelligence Technologies

CTM360®

Mapping the World's External Digital Risks

External | Consolidated | Technology, Data & Managed Services

Copyright @2026 **CTM360®**