Report | **July 2025**

BaitTrap

The Rise of Baiting News Sites behind online Investment Fraud

CTM360®

TLP: CLEAR

INDUSTRY All

COUNTRY All

REGION Global

DATE 08-07-2025

OVERVIEW :

Baiting News sites (BNS) is a tactic used by scammers to spread and promote investment fraud at scale. These sites are designed to look like legitimate news outlets, publishing fabricated stories that feature well-known public figures and respected financial institutions. The content is crafted to build trust and lure users into scams such as Trap10, Crypto trading fraud and other high-risk financial schemes.

Scammers push Baiting News sites through ad platforms like Google and Meta, these sites serve as entry points. Once users click on a fake news article, they are redirected to professionally built scam platforms that promise easy profits and high returns. In reality, these fake platforms are set up to deceive and defraud unsuspecting individuals.

To date, through its WebHunt platform, CTM360 has identified over 17,000 Baiting News Sites across 50 countries. These sites are often tailored to local audiences, using native languages, recognizable brands and regional public figures to appear more credible and increase their chances of scamming victims.

CTM360 continues to monitor, uncover emerging patterns and take action to reduce the spread of these Baiting News sites.

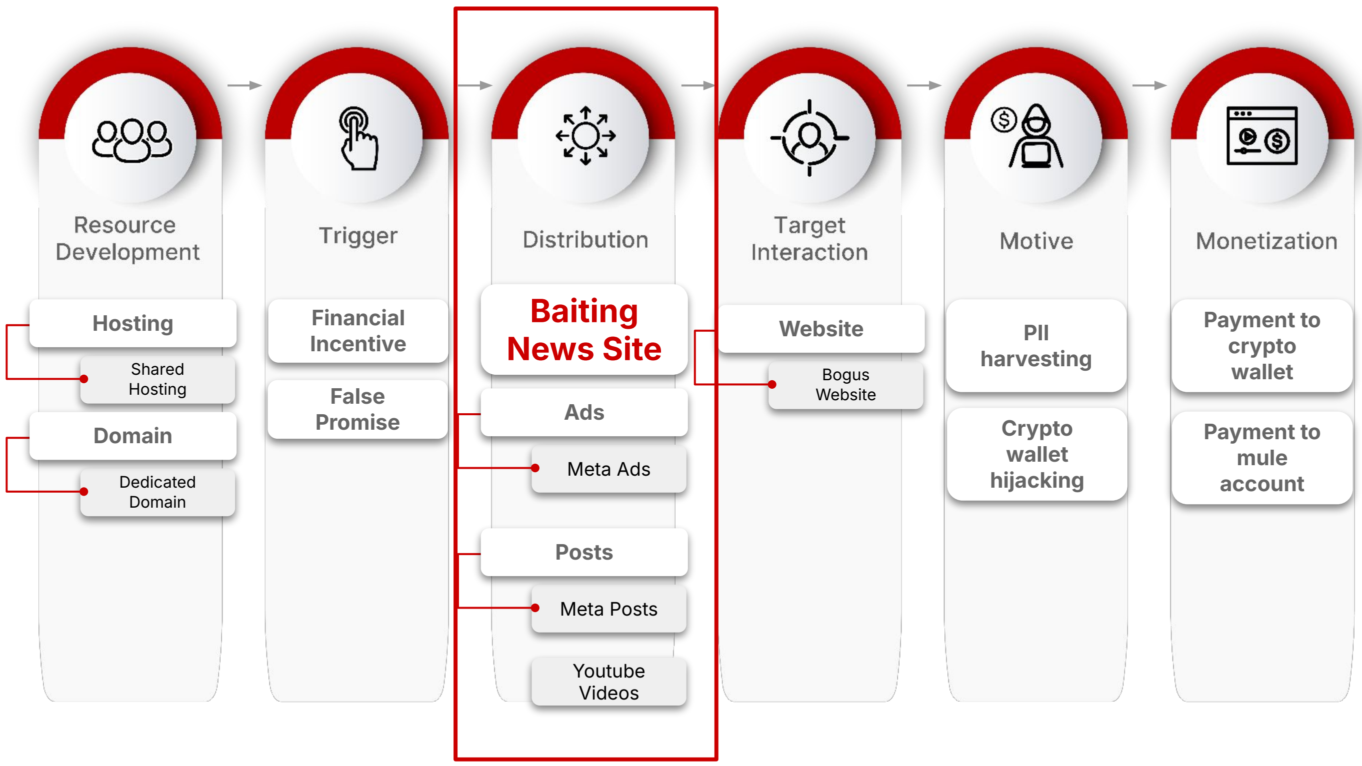
Key Findings on Baiting News sites

- Baiting News Sites are designed to mimic trusted global media outlets such as **CNN, BBC, CNBC, News24, and ABC News**. Over **17,000** of these sites have been identified to date, all redirecting users to fraudulent investment platforms.
- These sites publish fake stories that falsely link **public figures and financial institutions including National banks, Central banks, and Commercial banks** to fabricated investment schemes in order to build trust and get engagement from victims.
- Majority of Baiting News Sites have been observed using **free or low-cost top-level domains** such as **.xyz**, **.shop**, and **.click** etc.. In many cases, scammers compromise legitimate domains to host fake news pages, making detection and takedown more challenging.
- Baiting News Sites are often regionally tailored, using local languages, familiar media brands, regional banks and influencers to increase credibility.

SCAM STAGES:
CTM360 Scam Navigator

CTM360 Scam Navigator, inspired by the MITRE framework, is an analysis of the observed scams showing how the scammers navigate through different stages of the scam. Scam Navigator is a tool that categorizes common scam techniques, providing insights into typical patterns of fraudulent activity. Built on the MITRE model, it identifies six key stages in a scam: resource development, trigger, distribution, target interaction, motive, and monetization. There are commonly 2 phases in the scam, represented as Phase 1 (in white) & Phase 2 (in grey).

Highlighted in red, Baiting News Sites are used as a distribution technique. Scammers use them to initiate contact, build credibility and direct users toward fraudulent platforms designed to steal funds.

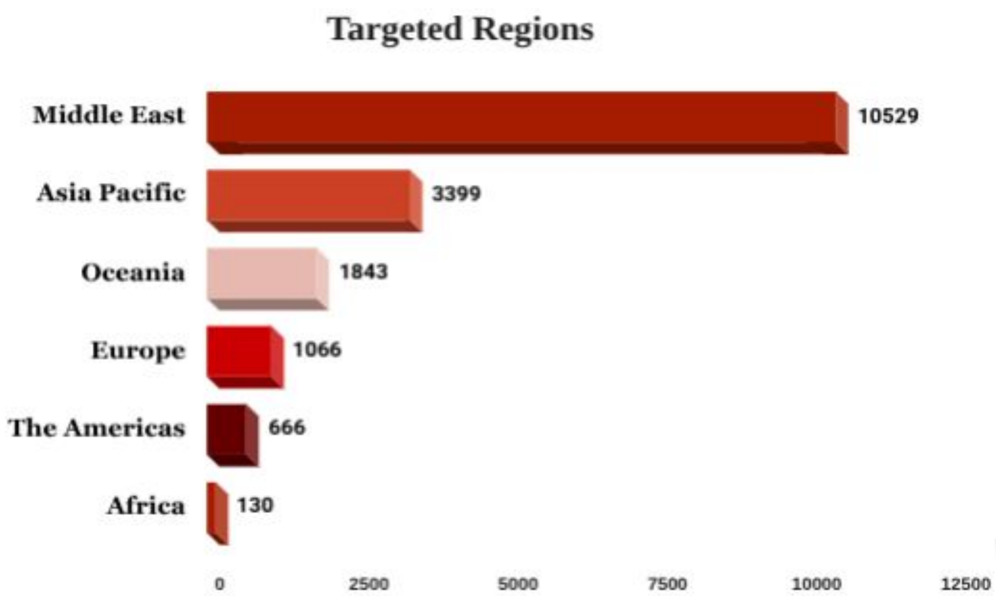


TLP: CLEAR

TARGETED REGIONS DISTRIBUTION

*Displayed below are graphs depicting the number of **Baiting News Sites** detected in different countries and regions*

Baiting News Sites



Top Targeted Regions

- Middle East
- Asia Pacific
- Oceania

Targeted Countries

- US
- China
- India
- Japan
- Germany
- UK
- France
- Brazil
- Canada
- Russia
- Italy
- South Africa
- Saudi Arabia
- Australia
- Indonesia
- 35 more...

TLP: CLEAR

CTM360®

CTM360 Observations

Fabricated stories falsely associated with well-known public figures with fake investment opportunities

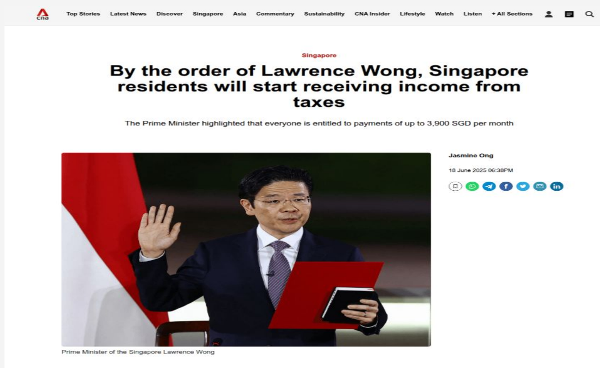
The screenshots below showcase sample templates of BNS across different regions

Middle East

Asia-Pacific

Europe

Oceana



Americas

Africa

17k+
Baiting News Sites

CTM360 Observations

Fabricated stories falsely associated with Central Banks, National Banks and Commercial Banks

Middle East

وزارة المالية:

تشارك وزارة المالية بنشاط في مراقبة المنصة والإشراف عليها لضمان مستوى عالٍ من أمان الأصول وحماية حقوق المستثمرين.

هذا المستوى من الشفافية والتحكم يجعل **استثمارات قطر للطاقة** خيارًا جذابًا لأولئك الذين يبحثون عن فرص استثمارية آمنة وموثوقة.

وزارة المالية
Ministry of Finance
State of Qatar • دولة قطر

قطر للطاقة
QatarEnergy

QatarEnergy Investments

وزارة المالية

كما أوضحت وزارة المالية أنه لضمان دخل مرتفع ومستقر لجميع المشاركين، سيكون هناك عدد محدود فقط من الأماكن المتاحة. حاليًا، المنصة مفتوحة لـ 5,000 شخص، ولم يتبقَ سوى 964 مكانًا!

Asia-Pacific

Bank of India

National Sort Code
93-13-14

Account name
Rahil Kumar

Telephone
01-8721022

Account number
18491-081

Page Number
33

Date of Statement
27.06.2025

1621A101

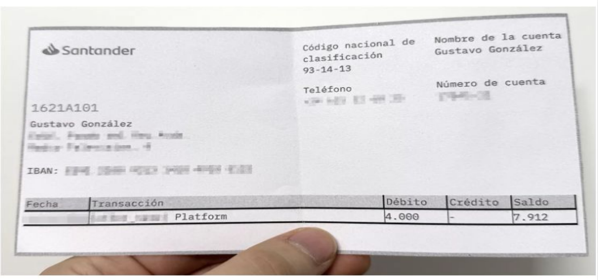
Rahil Kumar
Express Building, Block B1B
Sector 10, Noida 201301, UP

IBAN: IE67 AIBK 9313 1418 4910 81

Date	Details	Debit	Credit	Balance
21.06.2025	ONLINE WALLET	-	18.595	0
28.06.2025	IMMEDIATE LUMINARY	6.207	-	24.802
27.06.2025	IMMEDIATE LUMINARY	5.340	-	30.142
27.06.2025	ONLINE WALLET	-	5.200	25.142
26.06.2025	IMMEDIATE LUMINARY	17.472	-	42.614

Thank you for banking with us.

Europe



Un extracto bancario oficial que demuestre que el dinero ha sido acreditado Dinara Vaulten ¡realmente funciona! Si no hubiera retirado mis ganancias, estimo que esos 250 euros se habrían convertido en un millón después de 11 semanas".

Oceana

It will allow people to earn from $20,000 per month

29/06/2025 an innovative project by Andrew Forrest, Finance Legend, was launched in Australia. The country's authorities and the businessman had been preparing for its launch for four years.

Americas

RBC

Royal Bank of Canada
P.O. Box4047 Terminal A
Toronto ON MSWIL5

Your account number:
02064-574219556

Summary of your account for this period
RBC Day to Day Banking™ 02064-574219556

Royal Bank of Canada

Opening balance	**$1,053,027.21**
Total deposits into your account	**+ 284,582.01**
- Stock Investment Income	214.66
- Digital Investments ("Trading Platform")	284,367.35
Total withdrawals from your account (categories not specified)	**- 10,436.09**
Closing balance	**$1,327,173.13**

Attention:

All data is up to date and confirmed by the treasury service of the Royal Bank of Canada. The provided information is confidential and is not subject to public disclosure without the consent of the bank representative and the bank customer.

Africa

Sudden Call — Panic Hits the Studio!

At that moment, the producer's phone starts ringing frantically. It's a senior executive from **First National Bank (FNB)** — South Africa's biggest bank.

Voice on the phone (panicked, loud enough for nearby mics to pick up): *"Stop the broadcast IMMEDIATELY! You are destabilizing the financial system! This information could cause mass withdrawals and collapse financial markets!"*

Tshidi Madia (furious, shouting back into the phone): *"Of course they're scared! They're terrified ordinary people might finally make money WITHOUT their permission!"*

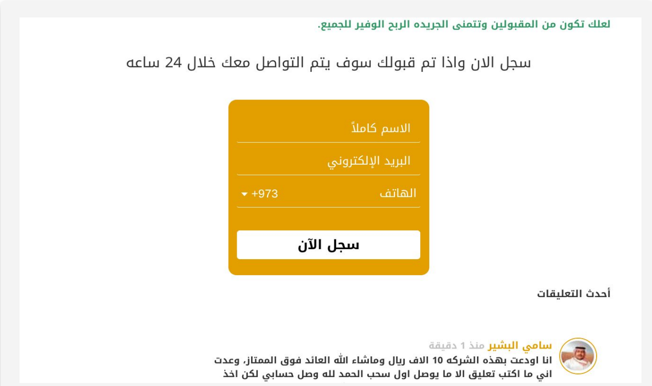
Voice on the phone (threatening): *"If you don't end it now, legal action will be taken against the channel."*

TLP: CLEAR

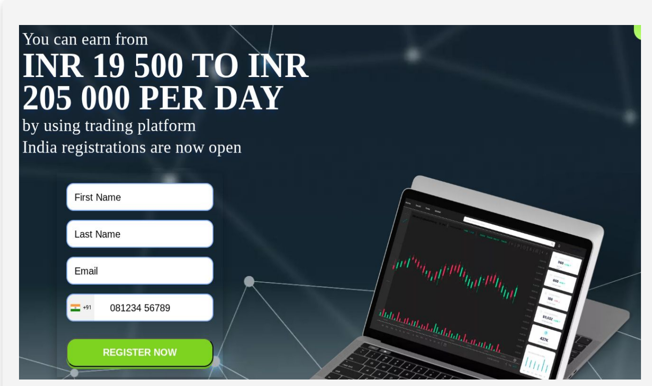
CTM360 Observations

The screenshots below showcase investment platforms from **BNS** across different regions **globally.** BNS redirects users to **investment platform (Trap10)**, which prompts individuals to submit their personal details and wait for a follow-up call from an "agent" to proceed.

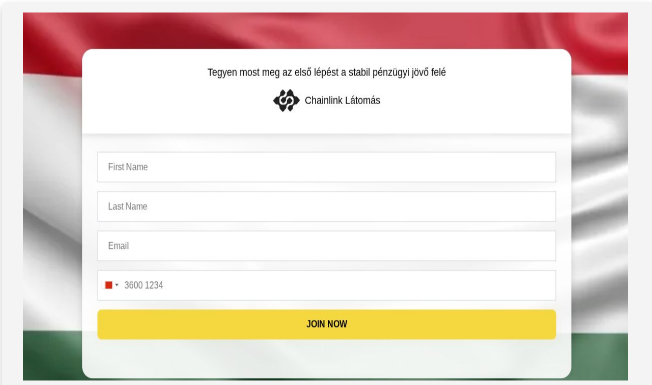
Middle East



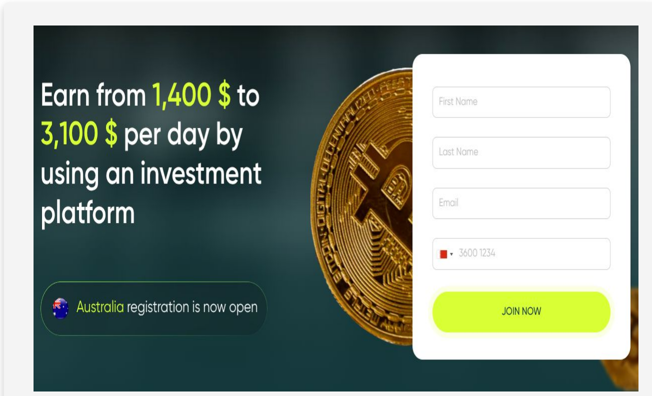
Asia-Pacific



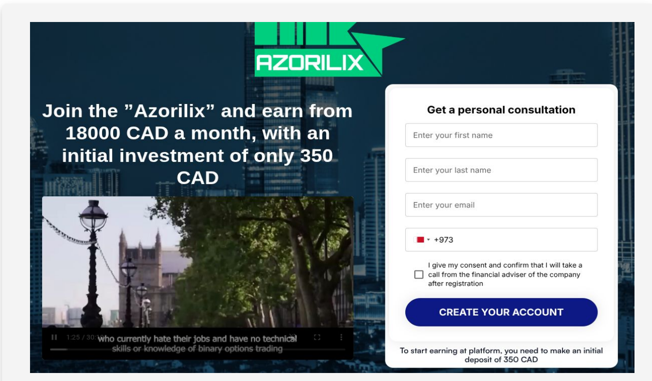
Europe



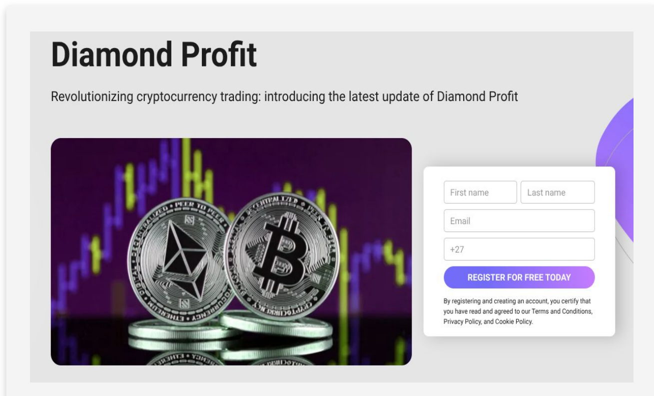
Oceana



Americas



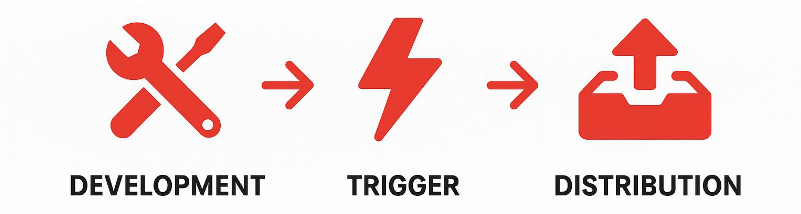
Africa



CTM360 Observations

Resource Development

Scammers set up the scheme using fake ads on Google Ads, Meta Ads, and social media. These ads lead users to fake news sites that falsely claim celebrities endorse a platform called "Eclipse Earn," supposedly an automated crypto trading service. In reality, it's a scam. Victims are shown fake profits to lure them into investing more, but no real trading happens. The money goes straight to the scammers. The fake sites and the "Eclipse Earn" platform are all designed to look legitimate, using fake testimonials and manipulated data to deceive users.



Trigger and Distribution

Scammers lure victims through sponsored ads on Google, Meta, and blog platforms, promoting fake news articles that impersonate trusted media outlets. These articles falsely claim that prominent public figures such as central bank governors or national leaders have accidentally revealed secret methods for generating wealth through crypto.

- **Google/Meta Ads:** Ads often use headlines like “You won’t believe what the [central bank governor] just revealed about making money from home,” paired with official photos or national symbols to increase credibility.
- **Baiting News Site:** Clicking the ad redirects to a fake news article designed to resemble CNN, Bloomberg, or local media outlets. These articles impersonate high-profile individuals and financial institutions, including central banks, and publish fabricated stories and quotes that suggest these entities endorse a platform called "Eclipse Earn" a supposed automated crypto investment system.
- **Fake Platform:** Victims are directed to a polished but fraudulent trading website. After signing up, they’re prompted to make a small initial deposit. The platform shows fake profit dashboards and fabricated returns, convincing users to invest more, even though no real trading takes place.

CTM360®

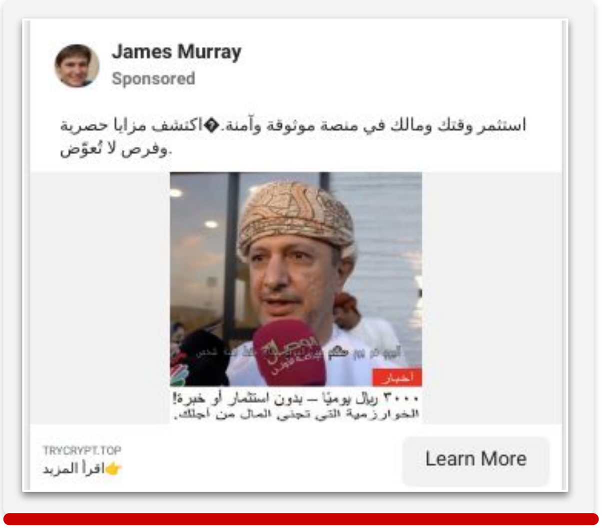
CTM360 Observations

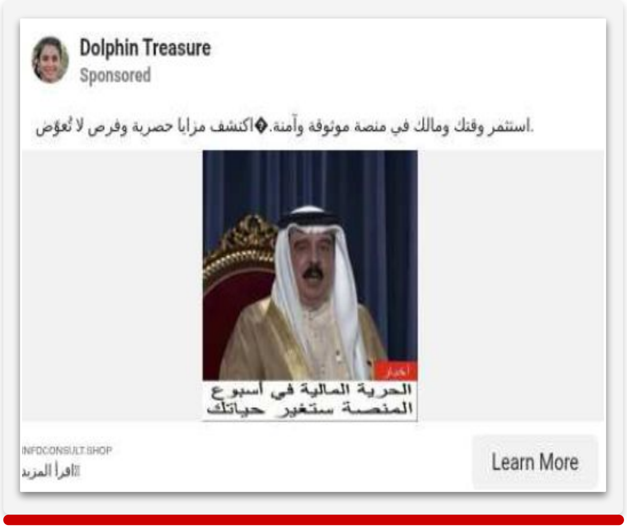
Target Interaction

Bogus Profiles & Meta Ads

Scammers use the same accounts, often with no history, zero followers, and minimal profile details, exclusively to host sponsored advertisements. These ads:

- **Photos of high-profile individuals:** The ads feature well-known public figures such as politicians, central bank officials, or celebrities to gain instant credibility.
- **Fake headlines that mimic news stories:** The ads promote claims like “Top official reveals new way to earn from crypto,” or “This platform lets anyone trade and earn daily income,” creating the illusion of legitimacy.



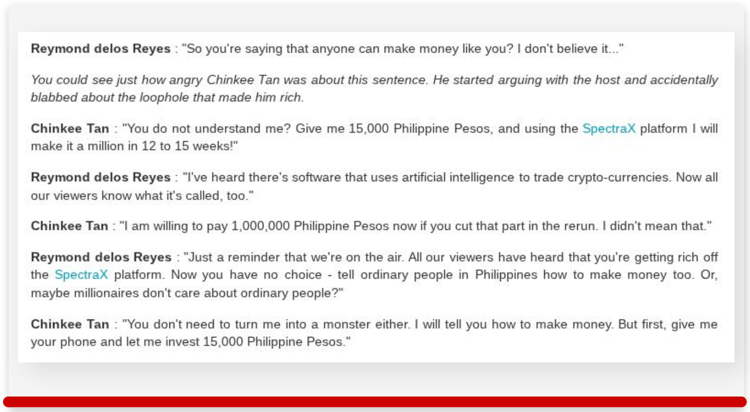


Samples of sponsored ads using well-knowns public figures

Fake Investment Registration Page

When a victim clicks on the ad or link to the platform, they are redirected to a fraudulent registration page—often branded to look like a legitimate trading service (e.g., "Trap10" or similar):

- **Personal Data Collection:** The page prompts the victim to enter personal information, including name, phone number, and email address, under the guise of account setup.
- **Follow-Up by “Expert Agent”**: Once submitted, the victim is told to expect a call from an investment “expert” or “advisor,” who will walk them through the next steps—typically pushing for an initial deposit to “activate” the trading account.



Reymond delos Reyes : "So you're saying that anyone can make money like you? I don't believe it..."

You could see just how angry Chinkee Tan was about this sentence. He started arguing with the host and accidentally blabbed about the loophole that made him rich.

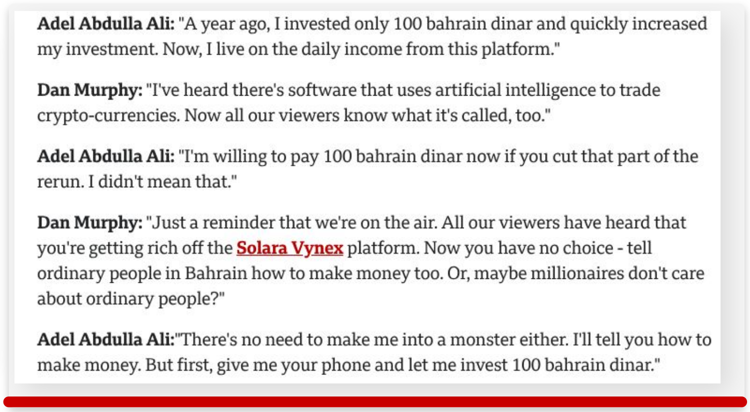
Chinkee Tan : "You do not understand me? Give me 15,000 Philippine Pesos, and using the SpectraX platform I will make it a million in 12 to 15 weeks!"

Reymond delos Reyes : "I've heard there's software that uses artificial intelligence to trade crypto-currencies. Now all our viewers know what it's called, too."

Chinkee Tan : "I am willing to pay 1,000,000 Philippine Pesos now if you cut that part in the rerun. I didn't mean that."

Reymond delos Reyes : "Just a reminder that we're on the air. All our viewers have heard that you're getting rich off the SpectraX platform. Now you have no choice - tell ordinary people in Philippines how to make money too. Or, maybe millionaires don't care about ordinary people?"

Chinkee Tan : "You don't need to turn me into a monster either. I will tell you how to make money. But first, give me your phone and let me invest 15,000 Philippine Pesos."



Adel Abdulla Ali: "A year ago, I invested only 100 bahrain dinar and quickly increased my investment. Now, I live on the daily income from this platform."

Dan Murphy: "I've heard there's software that uses artificial intelligence to trade crypto-currencies. Now all our viewers know what it's called, too."

Adel Abdulla Ali: "I'm willing to pay 100 bahrain dinar now if you cut that part of the rerun. I didn't mean that."

Dan Murphy: "Just a reminder that we're on the air. All our viewers have heard that you're getting rich off the Solara Vynex platform. Now you have no choice - tell ordinary people in Bahrain how to make money too. Or, maybe millionaires don't care about ordinary people?"

Adel Abdulla Ali:"There's no need to make me into a monster either. I'll tell you how to make money. But first, give me your phone and let me invest 100 bahrain dinar."

CTM360 Observations

Agent Contact & Data Harvesting

Upon completing the fake registration form, the scam proceeds with a phone call from an assigned "investment expert" who claims to assist with activating the account in order to begin trading.

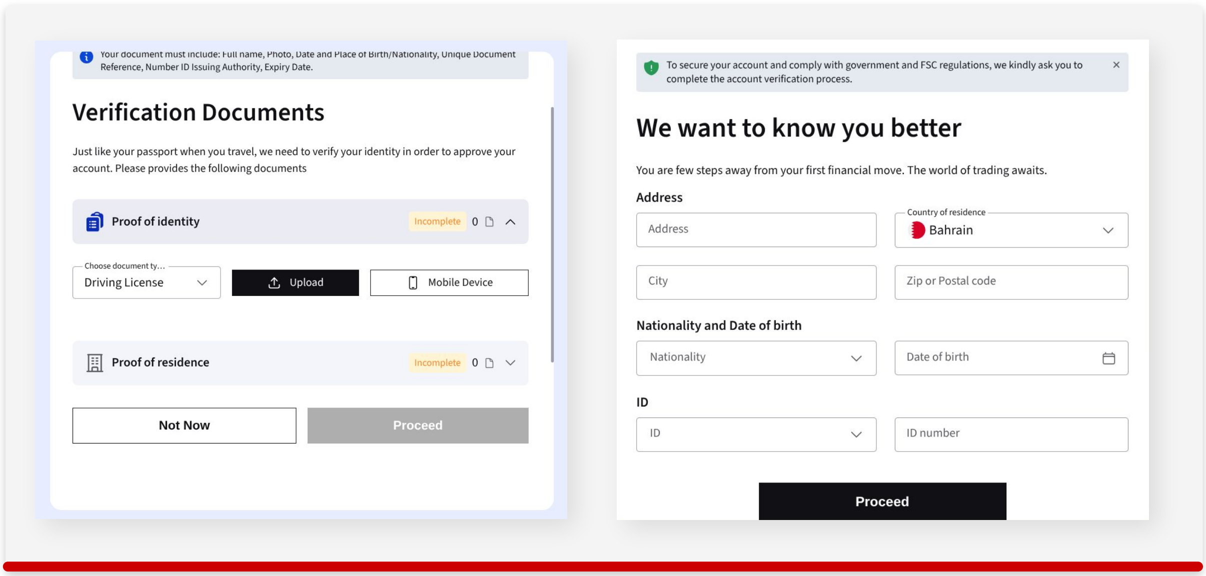
Personal Data Extraction: During the call, the agent requests sensitive personal details, including full name, phone number, email address, national ID, and banking information, under the pretext of verifying the user's identity and preparing the account.

False Sense of Legitimacy: The conversation is often scripted to resemble professional onboarding by financial institutions, creating trust and convincing the victim to comply.

Trading Platform Onboarding

After completing the registration, victims are directed to a fake trading platform branded as "Solara Vynex," or similar, designed to look like a legitimate crypto or investment portal.

- **Document Upload Requirement:** Before initiating any trades, victims are asked to upload identification documents—such as a national ID, passport, or proof of address—under the guise of account verification or regulatory compliance.
- **Account Funding Options:** To "activate" the trading account, victims are instructed to deposit funds using cryptocurrency wallets, credit/debit cards, Google Play gift cards, or direct bank transfers.
- **No Real Returns – Only Illusions:** While the platform may display fake account dashboards showing growing profits, no actual trading occurs. These figures are fabricated to deceive victims into making additional deposits, believing they are earning high returns.



CTM360 Observations

Motive

Financial Gain: Scammers engineer the scheme to extract deposits from as many victims as possible, pocketing the bulk of those funds.

Data Harvesting for Secondary Abuse: By collecting KYC-style information (ID numbers, bank details, contact lists), they build rich profiles to sell on the dark web or use in future phishing, social-engineering, or credit-fraud campaigns.

Monetization

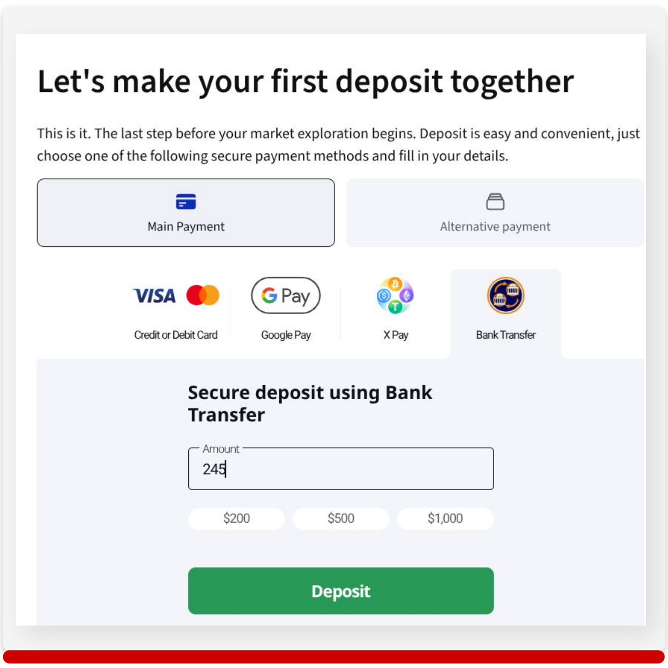
Initial Investment & False Trading Access

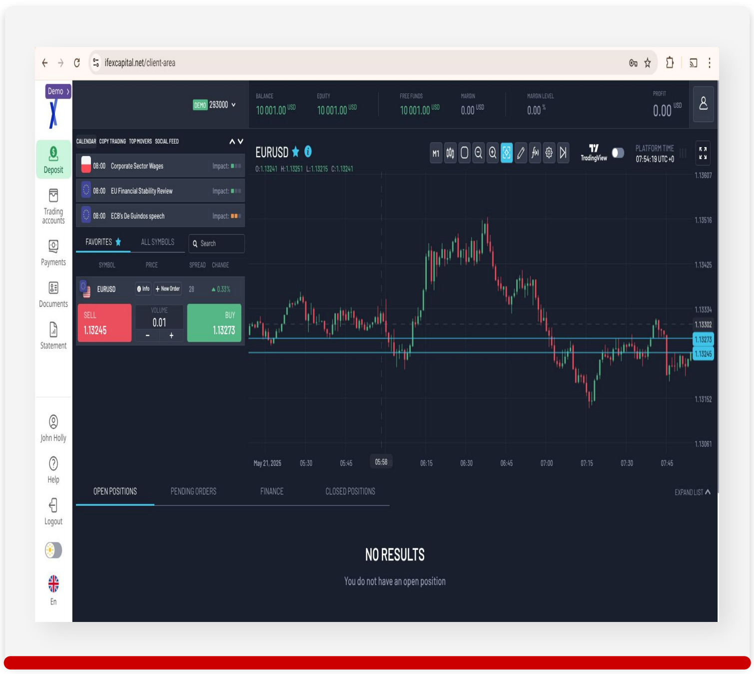
Victims are lured into making an initial deposit of around $240 to “activate” their trading accounts on fraudulent platforms such as Solara or Vynex. After payment, the platform simulates access to live trading dashboards, showing fake profit growth to reinforce legitimacy and encourage continued engagement.

Withdrawal Trap

Once the victim attempts to withdraw profits, the scam enters a new phase:

- Non-Functional Withdrawal Process: Despite visible “earnings” in the account, withdrawal options are disabled or delayed, citing issues like system errors, pending verification, or processing limits.
- Repeated Excuses for Delays: Victims are told they must complete additional verifications, pay unlock fees, or meet new “minimum balances” before the funds can be released.





ABOUT US

CTM360 provides a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and unlimited managed 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

CTM360 Community Edition Platform

Sign up today for free access to the
EASM + DRPS + Takedown + DMARC platform

Scan to Request Access
https://www.ctm360.com/free-access