# Exploration of the Dynamics of Buy and Sale of Social Media Accounts

Mario Beluri
mabe00023@stud.uni-saarland.de
Saarland University

Bhupendra Acharya
bhupendra.acharya@cispa.de
CISPA

Soheil Khodayari
soheil.khodayari@cispa.de
CISPA

Giada Stivala
giada.stivala@cispa.de
CISPA

Giancarlo Pellegrino
pellegrino@cispa.de
CISPA

Thorsten Holz
holz@cispa.de
CISPA

## Abstract

There has been a rise in online platforms facilitating the buying and selling of social media accounts. While the trade of social media profiles is not inherently illegal, social media platforms view such transactions as violations of their policies. They often take action against accounts involved in the misuse of platforms for financial gain. This research conducts a comprehensive analysis of marketplaces that enable the buying and selling of social media accounts.

We investigate the economic scale of account trading across five major platforms: *X*, *Instagram*, *Facebook*, *TikTok*, and *YouTube*. From February to June 2024, we identified 38,253 accounts advertising account sales across 11 online marketplaces, covering 211 distinct categories. The total value of marketed social media accounts exceeded $64 million, with a median price of $157 per account. Additionally, we analyzed the profiles of 11,457 visible advertised accounts, collecting their metadata and over 200,000 profile posts. By examining their engagement patterns and account creation methods, we evaluated the fraudulent activities commonly associated with these sold accounts. Our research reveals these marketplaces foster fraudulent activities such as bot farming, harvesting accounts for future fraud, and fraudulent engagement. Such practices pose significant risks to social media users, who are often targeted by fraudulent accounts resembling legitimate profiles and employing social engineering tactics. We highlight social media platform weaknesses in the ability to detect and mitigate such fraudulent accounts, thereby endangering users. Alongside this, we conducted thorough disclosures with the respective platforms and proposed actionable recommendations, including indicators to identify and track these accounts. These measures aim to enhance proactive detection and safeguard users from potential threats.

## 1 INTRODUCTION

With the widespread use of social media platforms and the growing number of users, fraudsters are increasingly exploiting platforms and their users with various social engineering tricks [28, 30, 51]. According to the Federal Trade Commission (FTC), scams originating from social media resulted in reported losses totaling $2.7 billion between January 2021 and June 2023 [44]. The report also highlighted that fraud originating from social media accounted for higher monetary losses compared to other methods of contact.

Scammers abuse social media users through sophisticated fraudulent schemes, often organized in a complex manner, and leverage a large number of fake accounts to add layers of sophistication to their attacks [63]. Beyond traditional abuses such as phishing [20], investment fraud [42], and impersonation [11], scammers are found to engage in various fraudulent schemes such as clickbait and engagement farming to generate revenue [29]; spreading manipulated news for political or financial gain [10]; using deepfakes or generative AI for romance scams or pig-butchering [35]; advertising counterfeit goods [62]; executing shipping scams [48]; fraudulent recruitment [47]; blackmail [41] and sextortion [46]; and influence campaigns to manipulate public opinion or trends [45]. These fraudulent schemes have escalated in scale operations in the last years, leading to unprecedented exploitation of social media platforms and their users.

Scammers likely find social media as an ideal platform for exploitation due to its ease of account creation compared to fake website setups. Account setup in social media profiles lacks steps such as purchasing domains and certificates or ensuring the domain does not get flagged. Social media accounts offer greater immunity compared to traditional attack vectors like email, phone, or websites. With the rise of websites that facilitate the *purchase* of social media accounts, scammers gain quick and credible entry points to exploit others. These pre-established accounts often come with out-of-the-box public metrics such as followers, likes, and interactions, making them appear authentic and trustworthy to potential victims. This *perceived legitimacy* enables scammers to carry out fraudulent activities with reduced suspicion. Furthermore, acquiring accounts with an existing audience allows scammers to bypass the effort of building followers organically, enabling them to scale operations rapidly.

These accounts also help evade platform detection by posing as genuine users, making it more challenging for social media platforms to identify and block malicious activities.

Our research is motivated by combining the above three key perspectives: (i) the growing number of social media users, (ii) the expansion and scale of scams on social media beyond traditional attacks, and (iii) the rise of websites selling social media accounts, which allow fraudsters to bypass effort, save time, scale operations, and evade platform detection. In this paper, we analyze the marketplaces that allow buying social media accounts. Our analysis provides a comprehensive study of the marketplaces and the accounts being sold, including their public engagement metrics and scam operations. Our work addresses the critical gap in understanding what happens when such accounts are purchased and how they are subsequently misused.

In this work, we perform a comprehensive evaluation of data collected from 11 marketplaces and over 38,000 accounts listed for sale. We analyze the processes sellers use to create accounts on these marketplaces, analyze how social media accounts are advertised and set up, and evaluate profile engagement metrics exploited for abuse. Furthermore, we quantify the impact and categorize the types of abuse associated with these accounts. Our work represents the first large-scale analysis of 11 marketplaces selling social media accounts of five platforms: *X* (formerly known as Twitter), *Instagram*, *Facebook*, *TikTok*, and *YouTube*. More specifically, we identified 38,253 accounts on five social platforms which resulted in over $64 million value for sale. We performed the tracking and comprehensive evaluation of 11,457 accounts that provided the links pointing to their respective social media platforms. Through evaluating account creation and post engagement from all five social media platforms, we shed light on how these accounts are later misused to target users. Additionally, we offer recommendations to mitigate such scams. In summary, we make following key contributions.

- We conduct the first large-scale empirical study of marketplaces involved in selling social media accounts, uncovering fraudsters targeting over 210 categories as part of their scams.
- We provide a comprehensive evaluation of profile engagement and account creation setups, identifying the operational scale and abuse categories in which these accounts are exploited to target platforms and their users.
- Finally, we propose recommendations and distill insights to combat such processes, aiming to prevent the emerging threats posed by these marketplaces and sold accounts.

To foster research, we share our code [56] related to marketplaces that were publicly advertised for selling. However, for data protection reasons, the data related to the study are only shared with interested academics, abused entities, or researchers upon request.

**Ethical Consideration and Data Disclosure.** Our research does not involve direct interaction with scammers or individuals, and relies solely on publicly available data. During data collection, we ensured that no engagement with human subjects occurred; our methodology was entirely passive and limited to publicly available data. Additionally, we disclosed relevant information, such as social media profiles, to all five social media platforms involved. For account-selling marketplaces, we ensured ethical compliance by refraining from bypassing CAPTCHAs, paywalls, evading automation triggers, and avoiding any direct interactions with social media profiles during automated data collection. Our findings were shared with all five social media platforms that we studied. We received positive feedback from X, expressing further interest in future collaboration.

## 2 BACKGROUND AND RELATED WORK

The proliferation of social media platforms has brought transformation changes to communication, entertainment, and business. However, alongside these benefits, social media has also become a fertile ground for abuse, fraud, and malicious activity. Bad actors exploit the platforms' vast user bases for illicit purposes such as account trading, spam, scams, and phishing, often causing harm to legitimate users and undermining trust in these platforms. Understanding the mechanisms and economic incentives behind these malicious activities is critical for designing effective countermeasures.

One growing area of concern is the emergence of fraudulent marketplaces that facilitate the trade of compromised or fake social media accounts. These accounts are used to amplify malicious campaigns, manipulate engagement metrics, or perpetrate fraud at scale. While previous studies have explored the broader cybercrime economy [22, 53, 57], little attention has been paid to the life cycle of these marketplaces and their accounts—from their sale to their eventual involvement in abuse, which we address in this work. We provide a framework for understanding the engagement and abuse patterns of these accounts after they are traded. Our work provides a comprehensive study of identifying accounts that are solid across various marketplaces and tracking the account's engagement and abuse categories. In the following, we discuss previous works related to our study and highlight our unique nature of work addressing the research gap.

**Cybereconomics and Fraudulent Marketplaces.** Some of the prior work that relates to ours focused on identifying malicious services or merchants and evaluating their business model and product offering over time [22, 53, 57]. Stringhini et al. [53] analyzed the operations of Twitter Account

Markets, which generate revenue by exploiting networks of followers, often through artificial inflation of follower counts or using compromised accounts to distribute promotional or abusive content. Similarly, DeKoven et al. [22] studied the for-profit services that drive traffic to manipulate the user's perception, while Thomas et al. [57] studied the role of the underground market in contributing towards abusive behavior such as scams and spams. However, none of these studies focus on identifying the accounts that are being sold and later tracking them to understand the maliciousness.

**Detection of fake accounts.** Another line of work similar to ours focused on the detection of fake accounts on social media, for example by constructing "social profiles" of users, allowing to detect discrepancies of the regular behavior (e.g., [19, 23, 50]) or by developing anomaly detection algorithms (e.g., [58, 61]). Further research developed detection techniques based on the characteristics of Twitter accounts and posts (e.g., [21, 31, 53, 55]), on the connections between profiles (e.g., [38]), or on the combination of multiple features (e.g., [13, 64]). Finally, Kurt et al. [57] studied patterns in the naming and registration processes of Twitter accounts, deriving patterns allowing to detection of abusive bulk registration of profiles. Our study differs from previous work, mainly in understanding the origination of the social media accounts that are later abused in scale.

**Spam, Scam, and Phishing.** Miscreants use social media platforms to spread spammy, malicious, or scam content [12, 19, 54], leveraging a post's content[24], visual appearance[52], or the reputability of a profile[20, 24], putting legitimate users at risk. Previous works measured the number of spam tweets and URLs, finding tweets containing over 2 million distinct URLs pointing to blacklisted scams, phishing, and malware over the period of two months [25], and showing that most accounts spreading malicious tweets are likely compromised [25], although new accounts are also registered specifically with this purpose. A similar study [24] conducted on Facebook confirmed this phenomenon, observing how compromised accounts are used to contact victim users posting URLs leading to advertisements, phishing, and drive-by downloads. Our work complements such studies by focusing on social media and various types of scams.

## 3 EVALUATION SETUP

In this section, we provide detailed information on evaluation setup and data collection process. Our evaluation framework consists of three main modules, as illustrated in Figure 1. Initially, we identify marketplaces that advertise the buying and selling of social media accounts (❶). Once identified, we curate these marketplaces based on the feasibility of data collection and proceed with semi-automated steps to gather advertised accounts. We then query the respective social media platforms to collect publicly available engagement and profile metadata linked to these advertised accounts (❷). Finally, we track and analyze the collected marketplaces and social media accounts to uncover the mechanics and operations behind these scams (❸). Below, we provide a detailed explanation of each of the three modules.

### 3.1 Collect Marketplaces

The market for buying and selling social media accounts is divided into public and underground markets. Public markets are accessible through standard internet searches and operate with a semblance of legitimacy, often hiding behind the guise of marketing services. In contrast, underground markets are clandestine, often accessible only via specific forums or onion directories on the dark web. These underground markets operate in secrecy to avoid detection and enforcement actions.

For data collection, we initiated our investigation through Google searches and a review of previous academic papers listing account-selling websites or underground markets [17, 22, 32–34, 43, 55, 57]. This preliminary research provided a foundation, which was further expanded by tracking postings in publicly accessible forums and onion directories that list underground market sites. This dual approach ensured a comprehensive understanding of both market types. This resulted in a comprehensive list of 58 websites and nine personal contact points (emails, phone numbers, telegram handlers). We focused on trading channels where social media account handles were publicly visible, excluding others from further automated data collection, as reported in Table 9 in the Appendix.

### 3.2 Data Collection

Our data collection relied on two primary sources: *(i)* accounts advertised by sellers on various marketplaces and *(ii)* for each account with a visible social media profile link, we queried the respective social media platforms to gather associated profile metadata and engagement posts. We provide further details below.

**Public Marketplace Account Collection.** We developed a JavaScript-enabled web crawler to automatically extract account-selling offers related to popular social media platforms. These include *X*, *Instagram*, *YouTube*, and *TikTok*. The crawler is implemented using *Python*, with *Selenium* for browser automation and the *Chrome DevTools Protocol* for fine-grained page control and interaction.

Each marketplace may have multiple listings covering various social media platforms, such as Instagram and Twitter. For each marketplace, we manually identified the seed URLs for different listings and initialized our crawler with

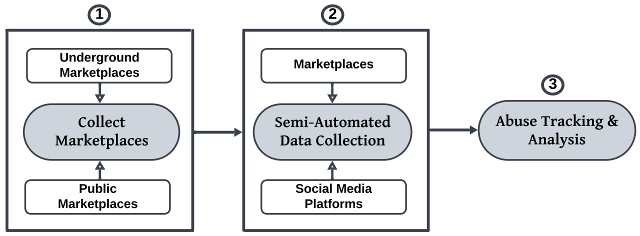


**Figure 1: Evaluation Setup – Our evaluation setup comprises three main modules. Initially, we collect marketplaces that sell social media accounts based on manual search (❶). Through semi-automation, we collect data from various marketplaces related to advertised accounts and further query social media APIs to collect data related to the advertised account (❷); finally, we evaluate the collected data by analyzing the marketplace, and their affiliated social media accounts including scam tracking and abusive elements associated with such accounts (❸).**

**Table 1: Overview of the public marketplace sellers and advertised social media accounts for sale. Among these 11 marketplaces, *Accsmarket* was found to have the highest number of advertised accounts, and *FameSeller* was the lowest.**

| Public Marketplace | Sellers | Accounts |
|---|---:|---:|
| Accsmarket | 2,455 | 13,665 |
| FameSwap | 6,617 | 8833 |
| Z2U | 240 | 6,417 |
| SocialTradia | - | 4,020 |
| InstaSale | 251 | 1,950 |
| MidMan | 304 | 1282 |
| TooFame | - | 695 |
| SwapSocials | - | 530 |
| SurgeGram | - | 205 |
| BuySocia | - | 547 |
| FameSeller | 77 | 109 |
| **Total** | 9,944 | 38,253 |

these URLs. Given a seed URL, the crawler employs a depth-first strategy: it visits a listing page, clicks on each offer to reach the offer webpage, and collects its details. This process continues until all offers on a listing page are covered. The crawler then moves to the next listing page and repeats the process, stopping only when no new offers or listing pages are found. For each advertised account for sale, we collect displayed information such as offer URL, title, seller information, price, payment methods, social media account handles, account properties (such as the number of likes and followers), and the offer description. Out of 58 trading markets, 11 contain selling offers with publicly visible social media account handles, which we focused on. In Table 1, we display each marketplace, seller, and advertised account detail. In total, we collected 38,253 URLs from the 11 marketplaces, out of which 11,457 URLs display accounts linked to respective social media platforms. Among these marketplaces, 35% (13,665/38,253) of accounts resulted from *Accsmarket* as the highest number of accounts, and the lowest accounted from *FameSeller* 109 accounts, lesser than 1% of the total accounts found. We identified, 5/11 marketplaces, *SocialTradia*, *TooFame*, *SwapSocials*, *Surgegram*, and *BuySocia* omitting the public display of seller's information.

**Profile Metadata Collection.** Of 38,253 advertised accounts from open marketplaces, 29% (11,457) of the accounts for sale advertised visible links pointing to their respective social media profile. For each of these social media accounts, we collected each profile's public profile metadata, including user profile names, descriptions, account creation dates, and engaging posts, from visible accounts linked to the advertised seller's marketplace page. For this, we utilized the respective API services [14–16, 39, 40, 59, 60] of the social media platforms. In Table 2, we present a detailed breakdown of the collected social media accounts and their corresponding posts. Our findings show that *YouTube* accounts had the highest number of visible account profiles linked, account 54% (6,271/11,457) of the total visible accounts, whereas the lowest count resulted from *Facebook*, 5% (649/11457) from our overall visible accounts.

**Underground Forum Account Collection.** We analyzed accounts sold on underground markets accessed via the Tor network. Initially, we manually inspected these markets to confirm their accessibility and available goods. Many markets referenced in related research were inaccessible due to takedowns, lack of directory listings, or timeout errors, while others were non-English, or did not sell digital goods. This narrowed our focus to four underground markets. We expanded our dataset by adding 16 more underground forums found in onion directories, which sold social media-related goods at the time of this first inspection. All inspected markets required user registration and implemented complex, site-specific, non-standard *CAPTCHAs*. Additionally, navigation was restricted: attempts to access pages not linked within the current page resulted in blocks. Due to these limitations, we collected all account sale data manually. Data collection followed two criteria: *(i)* browsing forum sections dedicated to accounts or social media, or *(ii)* using forum search functionalities with keywords like *[account/s | profile/s] [name of social media]*. In both cases, we recorded data

Table 2: Overview of the social media data collection. In the table, we display social media accounts advertised for sale. The accounts that are listed referencing the social media platform account profile we name them as visible accounts.

| Social Media | Visible Accounts | Visible Accts. Posts | All Accounts |
|---|---|---|---|
| Instagram | 2,023 | 4,207 | 12,658 |
| YouTube | 6,271 | 3,411 | 9,087 |
| Tiktok | 1700 | 25,131 | 8,973 |
| Facebook | 649 | 7,407 | 4,216 |
| X | 814 | 165,427 | 3,319 |
| **Total** | 11,457 | 205,583 | 38,253 |

from the first five pages of results, up to 25 postings per social media platform.

Of the 20 markets in our initial dataset, eight did not sell social media-related goods, and four offered services like likes and followers but no accounts, leaving a final dataset of eight underground markets. In the second manual inspection, we collected for each posting the URL, title, textual content, author's username, publication date, number of replies, price, quantity sold, and a screenshot. Differences in forum models and GUIs meant that not all fields were consistently available across forums. For example, some forums did not display the date when a message was posted, or disallowed comments under the listings.

## 3.3 Tracking and Analysis

The third module analyzes the data collected from marketplaces and analyzes the engaged posts from the advertised accounts. This includes aspects such as the intricacies of sellers' advertisements, public engagement with social media profiles, and abusive elements such as scam tactics and the operations of scammers targeting social media users.

We present our findings as follows: an overview of marketplaces in Section 4; profile creation and engagement analysis in Section 5; scam clustering and abuses in Section 6; tracking and network analysis on Section 7, efficacy and abuse control in Section 8 and finally we provide recommendation to fight against such scam in Section 9.

# 4 ANATOMY OF MARKETPLACES

We conducted a comprehensive analysis of both open and underground marketplaces involved in the buying and selling of social media accounts. Our motivation to study both types of marketplaces was to understand a broader spectrum of account trade ecosystems—ranging from visible, mainstream practices to hidden, and illicit operations. We provide detailed insights for each section below.

## 4.1 Anatomy of Public Marketplaces

In this section, we outline how sellers set up their profiles in public marketplaces to advertise their accounts. Specifically, we analyze into categories, account monetization, verification, descriptions, public metrics, and account pricing. We provide further detailed information as below.

**Seller.** We identified 9,949 sellers across 11 marketplaces. The highest number of sellers composite from *FameSwap* with 6,617 sellers, while 5/11 marketplaces *BuySocia*, *SocialTradia*, *SurgeGram*, *SwapSoul*, and *TooFame* lacked sufficient seller information. The median number of seller accounts was 77. Regarding seller nationality, 29,420 sellers did not disclose their country of origin, while 8,833 sellers represented 138 countries. Among these, the top five countries were the *United States* (2,683 sellers), *Ethiopia* (844), *Pakistan* (596), the *United Kingdom* (382), and *Turkey* (366). In Figure 2, we showcase the cumulative growth and activity of listings across the data collection iterations. Our observations suggest that accounts are replenished to align with supply and demand, ensuring readiness for future sales opportunities.

**Categories Analysis.** Out of 38,253 accounts, 22% (8,775) were found to lack any categorical representation. Among the remaining 29,478 advertised accounts, 212 unique categories were identified. The top five categories were *Humor/Memes* (5,056 accounts), *Luxury/Motivation* (2,292), *Games* (1,062), *Fashion/Style* (1,678), and *Reviews/How-to* (1,420). The median account size for these categories was 3.

**Verified Accounts.** Out of 38,253 accounts, we identified 185 with verified social media statuses, all of which were YouTube accounts. However, these accounts did not provide URLs linking to their respective YouTube channels. It is likely that sellers use this strategy to attract potential buyers.

**Account Monetization.** We identified 164 accounts reporting monthly revenue generation ranging from $1 to $922, with a median value of $136 and a total combined revenue of $42,019 per month. Some sellers provided additional details about income sources and the potential benefits buyers could gain from purchasing these accounts. In total, 1,020 sellers disclosed unique income sources. The top three narratives included: *(i)* generic ad-based revenue (335 sellers), *(ii)* Google AdSense (73 sellers), and *(iii)* video accounts with premium memberships or channel monetization (73 sellers). Examples of these narratives are provided below:

*The account generates income by selling promotion plans to nft and crypto projects. You can sell tweets, retweets or some*

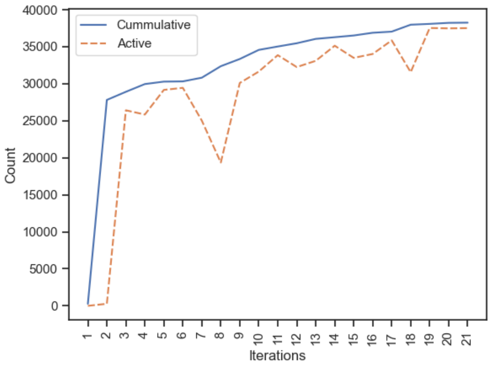


**Figure 2: In this graph, we present the cumulative and active listings advertised by sellers across 11 open marketplaces over our data collection iterations between Feb 2024 to Jun 2024. The decline in active listings suggests that some accounts went offline, possibly due to successful sales or the seller's decision to take them offline. At the same time, the continuous growth in cumulative listings, despite the dip in active ones, reflects the replenishment of inventory to maintain higher stock levels and meet supply and demand needs.**

*combos of boths. You can also sell weekly, middle or long term campaigns. A revenue-share is also a smart option. I can teach you everything to help you make income with my account.*

*You can monetise your content by selling promo videos or putting different watermarks on your Shorts videos for money.*

**Account Description.** Out of 38,253 accounts, 63% (24,293) included descriptions about the accounts. Through manual evaluation based on keyword analysis, we identified eight distinct strategies used in these descriptions: *(i)* listings labeled as authentic (784 accounts), *(ii)* listings labeled with "fresh and ready" accounts (157), *(iii)* listings promoting business adaptability (122), *(iv)* real user accounts with activity (116), and *(v)* offers with original email included. Examples of a description are shown below:

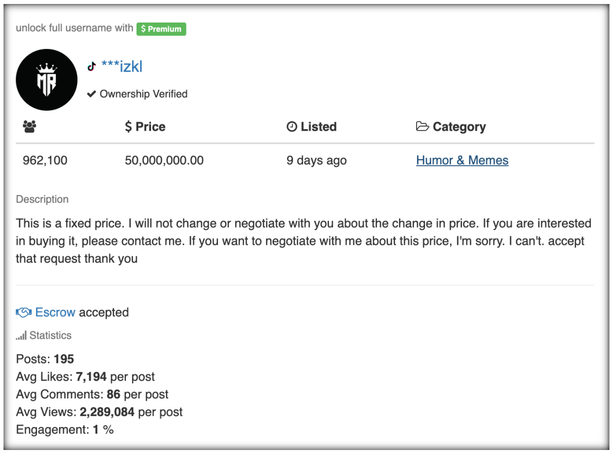
*No shout outs have ever been done on the account. So the account is fresh and ready for whatever purposes you need – CPA, product promotion + sales, drop shipping, traffic generation, or simply you want to own an Instagram page with real and active users. Save yourself time and energy of starting a new account and growing it (which can take months). Enjoy the convenience and time saved.*

**Table 3: Payment methods supported by different platforms.**

| **Payment Methods** | Accsmarket | FameSwap | Z2U | SocialTradia | InstaSale | MidMan | TooFame | SwapSocials | SurgeGram | BuySocia | FameSeller |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Traditional** | | | | | | | | | | | |
| Visa | | | ✓ | | | | | | ✓ | | |
| PayDirekt | | | ✓ | | | | | | | | |
| GPay Visa | | | | | | ✓ | | | | | |
| DLocal | | | | | | ✓ | | | | | |
| Appota Visa | | | | | | ✓ | | | | | |
| **Prepaid Vouchers** | | | | | | | | | | | |
| NeoSurf | | | ✓ | | | | | | | | |
| **Crypto** | | | | | | | | | | | |
| BTC | | | | | | ✓ | | ✓ | | ✓ | |
| ETH | | | | ✓ | | ✓ | | ✓ | | ✓ | |
| LiteCoin | | | | | | ✓ | | | | | |
| Tether | | | | | | ✓ | | | | | |
| BNB | | | | | | ✓ | | | | | |
| Matic | | | | | | ✓ | | ✓ | | | |
| Dash | | | | | | | | | | | |
| **Exchanges** | | | | | | | | | | | |
| Coinbase | | | ✓ | | | | | ✓ | | | |
| AirWallex | | | ✓ | | | | | | | | |
| **Digital Wallets** | | | | | | | | | | | |
| PayPal | | | ✓ | | | | | | | | ✓ |
| Trustly | | | ✓ | | | | | | | | |
| Skrill | | | ✓ | | | | | | | | |
| WeChat | | | ✓ | | | | | | | | |
| AliPay | | | ✓ | | | | | | | | |
| Payssion | | | | | | ✓ | | | | | |
| **Escrow-Based** | | | | | | | | | | | |
| Trustap | | | | | | ✓ | | ✓ | | | |
| Payer | | | | | | ✓ | | | | | |
| Unknown | ✓ | ✓ | | | ✓ | | ✓ | | | | ✓ |

*Selling TikTok account with over 2.1 million followers and a viral video with 69 million views and 13.5 million likes. The account averages millions of views per video. This account has proven to be highly engaging and has attracted a large following. If you are interested in purchasing this account, please free to make an offer.*

**Account Followers.** Advertised accounts often share their follower counts. We found that 40% (15,358) of accounts displayed follower information. The median follower counts for each social media platform were as follows: *X* (3077), *Instagram* (26,998), *TikTok* (20,807), *YouTube* (25,700) and *Facebook* (76,050).



unlock full username with $ Premium

***izkl

✓ Ownership Verified

| 👥 | $ Price | Listed | Category |
|---|---|---|---|
| 962,100 | 50,000,000.00 | 9 days ago | Humor & Memes |

Description

This is a fixed price. I will not change or negotiate with you about the change in price. If you are interested in buying it, please contact me. If you want to negotiate with me about this price, I'm sorry. I can't. accept that request thank you

Escrow accepted

Statistics

Posts: **195**
Avg Likes: **7,194** per post
Avg Comments: **86** per post
Avg Views: **2,289,084** per post
Engagement: **1** %

**Figure 3: An example of advertised seller accounts on *FameSwap* marketplace with exceptionally high prices, the reasons behind such elevated prices remain unclear. The account shows the follower count close million, and the price at $50 million.**

**Account Prices.** The median advertised prices for social media accounts were as follows: *Facebook* ($14), *X* ($17), *Instagram* ($298), *TikTok* ($755), and *YouTube* ($759). The overall sum of all advertised account prices totaled $64,228,836, with a median value of $7,573,348 across the platforms. Among the five platforms, *TikTok* had the highest total at $12,760,408, while *Facebook* had the lowest at $145,937. Although the reasons behind the exceptionally high pricing of some accounts remain unclear, 345 accounts were identified with prices exceeding $20,000. These accounts had a median price of $45,000, a maximum of $5,000,000, and contributed a total sum of $38,040,411. An example of such a price account is shown in Figure 3.

**Supported Payment Methods.** We analyzed the payment methods supported for buyers across 11 marketplaces. In Table 3, we present a detailed breakdown of these payment methods by the marketplace. Our findings indicate that cryptocurrency and digital wallets are preferred over traditional payment providers. This preference is likely rooted in their widespread adoption, enhanced anonymity, and reduced potential for disputes compared to traditional payment methods. In Appendix A, we provide additional detail in payment extraction and security implications.

## 4.2 Anatomy of Underground Marketplaces

Our investigation into underground markets for social media accounts began with an initial list of eight marketplaces: *Dark Matter* [3], *Kerberos* [4], *Nexus* [6], *Torzon Market* [8], *We The North* [9], *Black Pyramid* [2], *ARES Market* [1], and *MGM Grand* [5]. However, at the time of our in-depth data collection, we observed that two (namely *ARES Market* and *MGM Grand*) did not have any account for sale, leaving six markets for analysis. These provided valuable insights into the structure and dynamics of this illicit trade.

**Characteristics of the Marketplaces.** We collected a total of 65 posts from six platforms, related to four social networks. The *Nexus* market offers the largest amount of accounts (37), followed by *We The North* (15). The remaining four lists five or fewer accounts each, suggesting a lack of requests for this specific digital good. Listings in these markets describe accounts for sale emphasizing characteristics like follower counts, and engagement metrics (likes and views), specifying whether they are organic or bots, whether accounts are aged, and whether they are empty or populated with content. Posts can either sell single accounts or a bulk package, sometimes creating a mismatch between the listing price and the price per account. The six marketplaces displayed varying levels of activity and specialization. *Kerberos* had two sellers offering 51 accounts, primarily for *TikTok* and *X*, indicating a focus on bulk sales. The remaining markets offered one account per post. Dark Matter hosted five posts offering accounts for *YouTube*, *TikTok*, and *X*, from three sellers. *Nexus*, the most active market with 37 posts from four sellers, catered to *Instagram*, *X*, and *TikTok*. In the *Torzon* market, two sellers listed four accounts across *Instagram*, *TikTok*, and *YouTube*, and in *Black Pyramid* two sellers offered two *YouTube* accounts in two posts. *We The North*, with 15 posts from one single seller, exclusively targeted *TikTok*, emphasizing its prominence in the underground trade. Among the sellers, we identified two using the same username across platforms, suggesting cross-platform operations to maximize visibility.

**Structure and Content of Listings.** Listings generally featured concise descriptions, with post lengths averaging between 14 and 123 words depending on the market. Sellers included contact details such as Telegram handles or website links for payment and fulfillment, as marketplaces do not handle transactions directly. Posts also frequently outlined delivery logistics, guarantees, and disclaimers about seller liability, such as for lost credentials. On the other hand, listings almost never reported the handle of the advertised product (observed only once). Comment threads often included buyer feedback, trial requests, or "bumps" from sellers to increase visibility. Occasionally, buyers left testimonials confirming successful transactions.

**Patterns of Similarity Across Listings.** A significant pattern in our analysis is the high degree of similarity observed across some posts, with word similarity ranging from 88% to 100%. This repetition often involves the same username (or seller) reusing identical content for multiple posts, either on a single platform or across different platforms. Interestingly, the phenomenon is even more pronounced between sellers with distinct account names, particularly within the same marketplace, and to a lesser extent across different marketplaces.

TikTok-related offerings on the Nexus market exhibit the most notable cases of textual reuse. We carried out a case-insensitive similarity analysis after removing numbers and punctuation. For instance, we identified the same author using identical body text for two different posts (100% similarity), seven posts from three distinct sellers with highly similar content (average similarity of 98%), and two posts by the same seller on separate platforms, with identical text. Additionally, we found a single instance of two distinct authors posting identical text on different platforms. Altogether, 12 of the 42 posts analyzed displayed such high similarity, with all cases linked to just three authors. This consistency may suggest a coordinated effort rather than random duplication. Similar patterns were also identified for other platforms, though less frequently, with 2 out of 13 reused posts linked to Instagram (also involving the Nexus marketplace), 1 out of 3 for Twitter, and 3 out of 7 for YouTube.

## 4.3 Comparative Summary

Our observations on underground and open marketplaces showed that *(i)* underground forums are restricted via dark-web; *(ii)* sellers are not very informative and often operate under pseudonyms, whereas those on open marketplaces typically disclose limited identity information; *(iii)* the number of listings advertised in underground were less than 100, while the listings on open marketplaces found to be over 38K; *(iv)* listings on underground markets are ultimately similar to forum posts, resulting in sparse or missing information about account details (likes, followers); *(iv)* payments on underground markets were never handled by the platform but agreed upon on a different channel between buyer and seller, also via escrow methods, while payment methods on open marketplaces were rather flexible in types of payment methods; *(v)* the prices on underground markets can be unclear when purchasing in bulk, or in case of private bargaining or auctions, while the open marketplace found to contain pricing detail; and furthermore we observe there are no buyer-seller mediatory transactions involved thus buyer may find unprotected during purchase at underground marketplaces.

For the rest of the paper, our analysis of social media profiles will be based on the public marketplaces.

# 5 ACCOUNT SETUP AND ENGAGEMENT

In the previous section, we analyzed the anatomy of marketplaces and explored how accounts are advertised for sale.

**Table 4: Followers - In this table we present followers minimum, media, and maximum count based on the publicly marketed available social media accounts that contain visible profile URLs to respective social media platforms. We queried each social media account and obtained public metrics such as followers. This indicates that accounts for sale often harvest large numbers of followers.**

| Social Media | Min | Median | Max |
|---|---:|---:|---:|
| TikTok | 0 | 1 | 6,893 |
| X | 55 | 2,752 | 1,078,130 |
| Facebook | 115 | 27,669 | 5,239,529 |
| Instagram | 1032 | 8,362 | 6,288,290 |
| YouTube | 0 | 8,460 | 20,500,000 |
| **All** | 0 | 7,830, | 20,500,000 |

In this section, we focus on understanding how the strategic preemptive tailoring of profiles aligns with market demand. Based on our findings, these accounts are meticulously crafted to target specific categories by leveraging factors such as naming conventions, descriptions, geo-locations, account setup types, and creation dates. Our analysis reveals that the preemptive tailoring of profiles aims to mimic organic profiles, drive engagement, and build a substantial subscriber base. We provide detailed observations below

**Account Name and Description.** We observe profiles frequently adopt terms and themes associated with popular industries and interests, likely to attract a wide audience or to foster trust and credibility for malicious use. This includes, for example, *(i)* trendy terms such as crypto or NFTS (e.g., Crypt Hunter), *(ii)* names implying expertise or status (e.g., Mr. NFT expert), *(iii)* personalization appealing to specific demographics (e.g., Kajal Kumar), *(iv)* profile with the adult or sensitive theme (e.g., Massage in Riyadh), and *(v)* mix of unrelated names, emojis, or terms from regional and local languages (e.g., まんちカビゴン). The account naming inclusion of financial and gaming terms indicates likely targeting of users interested in fast wealth-building or entertainment.

**Location.** We identified 3,236 profiles that listed 140 unique locations as part of their profile address, although location entries are optional on social media profiles. Among these, the top five countries represented are the *US* (1,242), *India* (470), *Pakistan* (222), *South Korea* (156), and *Bangladesh* (114). This indicates that the US is the preferred location for account creation, potentially making the profiles appear more relatable and trustworthy to victims based on their origin.

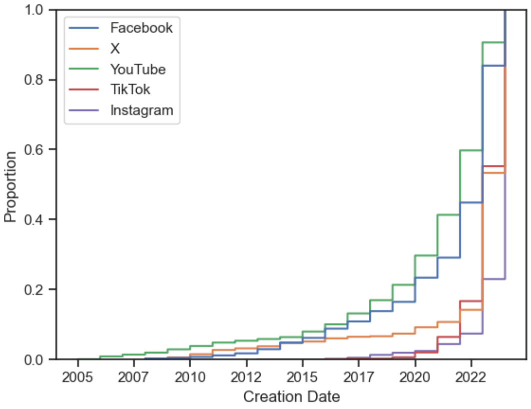


**Figure 4: Date of account creation - In this graph, we display visible social media account profiles from 5 social media platforms based on their date of creation date. We identify that 30% of accounts were created before 2020, and less than 0.5% of accounts from YouTube were created between 2006 to 2010.**

**Affiliated Categories.** Our observation showed that social media profiles were often tagged with platform-specific categories based on their relevance. We identified 288 distinct categories associated with 1,171 accounts. The top five categories include (i) *Brand and Business* (751), (ii) *Entities* (349), (iii) *Interests and Hobbies* (322), (iv) *Digital Assets & Crypto* (334), and (v) *Events* (219). Since categories like business, interests, and assets naturally attract public engagement due to their economic relevance, such accounts are likely to be in high demand in marketplaces for purchase.

**Account Types.** Social media accounts by default are unverified and lack restrictive settings such as protected or private modes. We identified three account types across five social media platforms: *(i)* business profiles marketed as entities (193), *(ii)* verified accounts (669), and *(iii)* accounts with controlled settings, including private (65) and protected (5) modes. This indicates that accounts for sale are predominantly unverified or standard profiles, with relatively fewer business or restricted accounts available.

**Account Creation.** Account creation dates provide insight into the age of social media profiles. In Figure 4, we present the CDF of account creation dates across five social media platforms. Our analysis reveals that over 70% of accounts were created within the last 3.5 years, while less than 25% were created between 2005 and 2020. Among the platforms analyzed, *TikTok* profiles were created between 2017 and 2024, while *X*, *Instagram*, and *Facebook* accounts date back to 2010. Notably, less than 0.5% of *YouTube* accounts were created between 2006 and 2010. This suggests that the majority of accounts advertised on these marketplaces are relatively new, with a smaller portion representing older, more established profiles.

**Followers.** Followers on social media platforms represent individuals subscribed to an account to receive notifications and view its content in their news feeds. Our analysis across five social media platforms shows that the median number of followers for accounts on sale exceeds 7,000, with the highest follower count surpassing 20 million. In Table 4, we present the minimum, median, and maximum follower counts for these accounts. This indicates that accounts marketed on such marketplaces are often highly engaged and likely employ engagement farming techniques to attract a substantial number of followers.

## 6 SCAM POST ANALYSIS

We perform a comprehensive evaluation to detect scam patterns given the 205K collected posts of 11.4K social media accounts (see Table 2). Our objective in analyzing these posts is to understand how fraudsters attract victims by performing various social engineering tricks. For this, we applied topic modeling techniques to group them into distinct clusters, and later performed a manual qualitative analysis of all resulting clusters to identify the scam clusters. In total, we identified six clusters performing fraudulent activities via posts.

**Technical Setup.** Beginning with the collected posts, we focus on those based on English text, for which we rely on the CLD2 library [18], and remove stop words using the BERTopic library [27]. Then, we extract embeddings for each post using the all-mpnet-base-v2 sentence transformer model [7, 49]. Lastly, we use HDBSCAN [36] and UMAP [37] for clustering, followed by the KeyBERT model [26] to identify potential scam posts and refine topic representations within each cluster. We then manually analyze the resulting clusters, arranged by their size, to identify types of scam offers, and provide details on security risks. We exclude clusters that do not contain scams from our study.

**Scam Findings.** Starting with the dataset of 205K posts, we applied our methodology outlined above to automatically group the posts into 86 distinct clusters. From each cluster, we randomly selected and manually analyzed 25 sample posts to assess whether the content within the cluster was related to scams. As a result of this vetting process, we identified 16 clusters containing scam-related content, which we further categorized into six overarching scam types.

Using this approach, we identified a total of 18.7K scam posts across over 3.7K distinct scammer accounts from five social media platforms: *Facebook*, *Instagram*, *Tiktok*, *X*, and *Youtube*. Table 5 provides a detailed breakdown of identified scam accounts and posts, and Table 6 presents a quick

**Table 5: Summary of scam accounts and scam posts identified across major social media platforms. Notably, YouTube had the highest number of scam accounts, while X led in scam-related posts, highlighting significant variations in the scale of fraudulent activity across platforms.**

| Social Media | Scam Accounts | Scam Posts |
|---|---:|---:|
| Facebook | 512 | 3,838 |
| Instagram | 525 | 3,271 |
| Tiktok | 461 | 3,034 |
| X | 610 | 6,988 |
| Youtube | 1,661 | 1,661 |
| **Total** | 3,769 | 18,792 |

**Table 6: Type and popularity of fraudulent offers across scammer's social media posts - This table presents six scam categories identified through post clustering. Our findings reveal that scammers frequently exploit trending topics and financial schemes, such as crypto/NFTs, while traditional scams like phishing, product fraud, adult content, and impersonation remain common.**

| Category | Accounts | Posts |
|---|---:|---:|
| **Financial Scams** | 2,649 | 8,903 |
| - Crypto Scams | 2,352 | 8,218 |
| - NFT and Giveaway Scams | 163 | 389 |
| - Financial Consulting | 81 | 133 |
| - Emotional Exploitation (Charity) | 53 | 163 |
| **Phishing** | 933 | 2,293 |
| - Through Popular Content/Challenges/Trends | 725 | 1,749 |
| - Through Chat Communication | 208 | 544 |
| **Product/Service Fraud** | 701 | 2,009 |
| - Product Promotion Scams | 296 | 739 |
| - Fake Travel Deals | 131 | 357 |
| - Vehicle Sale/Rental Fraud | 101 | 279 |
| - Sports Betting and Merchandise Scams | 129 | 451 |
| - Fake Education-related Offers | 44 | 183 |
| **Adult Content** | 244 | 466 |
| - Provocative and Catphishing Lures | 244 | 466 |
| **Impersonation** | 188 | 392 |
| - Public Figures | 53 | 133 |
| - Fake Tech Support | 135 | 259 |
| **Engagement Bait** | 2,300 | 4,597 |
| - Like/Follow/Subscribe Requests | 1,509 | 2,999 |
| - Greetings and Motivational Phrases | 791 | 1,598 |

overview of the scam categories. Below, we provide an in-depth analysis of the identified scam types.

**Financial Scams.** Financial scams are one of the most pervasive forms of fraudulent activity on social media, characterized by their focus on exploiting users' financial interests or vulnerabilities. These scams are perpetrated by 2,649 accounts producing 8,903 posts. A major subcategory is crypto scams, which involve promises of high returns on cryptocurrency investments, fake trading platforms, and fraudulent initial coin offerings. These scams leverage the rising popularity of digital assets to deceive users and account for 2,352 accounts and 8,218 posts. Similarly, NFT and giveaway scams capitalize on the emerging non-fungible token market by promoting fake NFT projects or false giveaways, engaging 163 accounts and 389 posts. Financial consulting scams target users seeking financial advice, with scammers impersonating consultants to extract sensitive information or money; this subcategory is responsible for 81 accounts and 133 posts. Finally, emotional exploitation scams, such as fake charity campaigns, manipulate users' goodwill by soliciting donations for fabricated causes, with 53 accounts and 163 posts contributing to this deceitful practice.

**Engagement Bait.** Engagement bait scams exploit users' desire for connection and social media algorithms that reward interactions. These scams involve 2,300 accounts generating 4,597 posts designed to maximize user engagement under false pretenses. Like/follow/subscribe requests, the most common type, are generated by 1,509 accounts through 2,999 posts. These requests often promise rewards or exclusive content in return for likes or follows but deliver nothing of value. Similarly, greetings and motivational phrases—posted by 791 accounts through 1,598 posts—capitalize on users' emotional responses to generic but engaging content. While appearing harmless, these tactics often serve as precursors to more deceptive practices by increasing scammers' visibility and reach.

**Phishing Scams.** Phishing scams are highly deceptive and aim to extract sensitive personal information such as login credentials, financial data, or identification details. These scams involve 933 accounts across 2,293 posts. One variant, phishing through popular content, challenges, or trends, mimics viral posts to lure users into clicking malicious links, with 725 accounts producing 1,749 posts. Another common form, phishing through chat communication, involves scammers directly messaging users while posing as trusted entities, accounting for 208 accounts and 544 posts. These scams exploit users' trust and curiosity, often leading to compromised accounts or financial losses.

**Product/Service Fraud.** Product and service fraud involves the false advertising of goods or services that do not exist, luring users with appealing offers. This category comprises 701 accounts generating 2,009 posts. Service and product promotion scams, executed by 296 accounts through 739 posts, mislead users with fake products, often using urgency to compel immediate purchases. Fake travel deals target vacationers with unrealistically cheap travel packages, involving 131 accounts and 357 posts. Vehicle sale/rental fraud, often associated with nonexistent cars or rentals, is perpetuated by 101 accounts through 279 posts. Additionally, sports betting and merchandise scams, conducted by 129 accounts through 451 posts, exploit sports fans with promises of exclusive merchandise or fixed betting outcomes.

**Adult Content Scams.** Adult content scams exploit the intimate nature of social media interactions to deceive users, often involving provocative imagery or fabricated romantic advances. These scams are carried out by 244 accounts across 466 posts. A typical scheme involves catfishing, where scammers pretend to be romantic interests to extract money, gifts, or sensitive information from their targets. These scams prey on users' emotions and can escalate into extortion or identity theft.

**Impersonation.** Impersonation scams rely on mimicking trusted entities, such as public figures or technical support services, to deceive users. This category includes 188 accounts generating 392 posts. Public figure impersonation, carried out by 53 accounts through 133 posts, involves scammers posing as celebrities or influencers to promote fake products or investment schemes. Similarly, fake tech support scams, conducted by 135 accounts through 259 posts, impersonate legitimate support agents to trick users into granting remote access to their devices or paying for unnecessary services. These scams exploit trust and authority to gain victims' compliance.

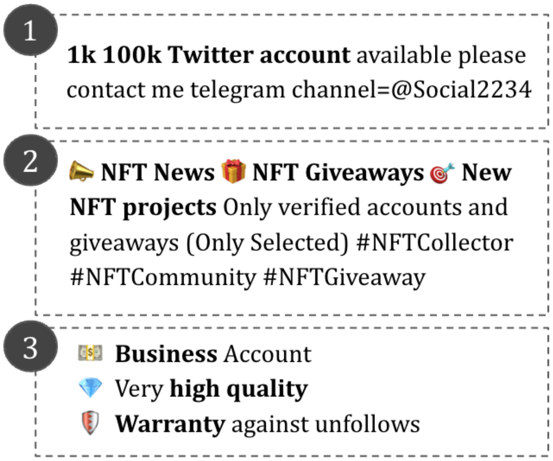
## 7 TRACKING AND NETWORK ANALYSIS

Our network analysis of visible profiles analyzes how account formations are linked to various other social media profiles enabling us to understand the scale of the operations. We provide network evaluation below.

**Cluster Formation.** To identify cluster formations, we selected profile metadata attributes such as names, descriptions, email addresses, websites, and phone numbers. Using these attributes, we automated the clustering process to group accounts from each social media platform into buckets containing at least two or more unique UserIDs. Accounts without matching attributes across multiple profiles were categorized as singletons. After the automated clustering, for each cluster of the cluster, we perform a manual inspection to validate the legitimacy of the groupings based on these attributes. Our findings are summarized below.

**Findings.** Our findings indicate that fewer than 5% of accounts were part of coordinated clustered campaigns. The remaining 95% of accounts showed no significant correlation with other social media profiles based on their visible profile metadata. In Table 7, we detail the clustering results for each social media platform, including cluster attributes, cluster sizes (minimum, median, and maximum), the total number of clusters identified, number of cluster accounts, singleton, and overall cluster accounts percentage from the dataset of each social media profiles from their respective platforms. Across the five social media platforms, a total of 203 clusters were identified, with the highest number of cluster composite from *YouTube*, and the lowest number of clusters from *TikTok*. Our observation showed that one of the clusters from *Instagram* consists of 46 social media accounts. The median and minimum cluster size across all platforms was 2, while the total median number of clusters identified across the five social media platforms was 35, containing a median of 89 accounts per cluster.

**Figure 5: Three examples of the profile descriptions of advertised social media accounts.**



1

**1k 100k Twitter account** available please contact me telegram channel=@Social2234

2

📣 **NFT News** 🎁 **NFT Giveaways** 🎯 **New NFT projects** Only verified accounts and giveaways (Only Selected) #NFTCollector #NFTCommunity #NFTGiveaway

3

💵 **Business** Account
💎 Very **high quality**
🛡️ **Warranty** against unfollows

We provide three illustrative examples of clustering based on the profile descriptions of advertised social media accounts in Figure 5. The first example illustrates the seller harvesting 1K accounts each of those accounts having 100K X (Twitter) followers and asking users to communicate via an external communication channel (Telegram), indicating a covert and significant scale of operations designed to engage victims privately. In the second example below, an account advertises free giveaways related to NFTs, which are used as bait to lure users into scams under the guise of community engagement. The third example shows an account targeting businesses or entities, offering high-quality profiles to attract buyers in the guise of established business or promotional purposes. Thus, these show a diversity of operations, ranging from large-scale scams to targeted strategies for monetizing social media accounts, and tactics employed by sellers beyond the originated marketplaces.

**Table 7: Network Cluster Detail - In this table we provide the network analysis of social media that contain shared attributes such as name, description, biography, email, phone,e or website. Based on their profile data analysis, we cluster the accounts by these attributes and present the clustering evaluation. Our results highlight that a single cluster from *Instagram* consists of as many as 46 social media accounts linked, whereas the smallest number of clusters consists of *TikTok*.**

| Social Media | Cluster Attributes | Min | Max | Median | Clusters | Cluster Accts. | Singleton | Overall Cluster Acts. |
|---|---:|---:|---:|---:|---:|---:|---:|---:|
| TikTok | Description | 2 | 22 | 4 | 3 | 26 | 1,674 | 1.5% |
| YouTube | Name | 2 | 3 | 2 | 97 | 195 | 6,076 | 3.1% |
| Instagram | Biography | 2 | 46 | 2 | 31 | 152 | 1,871 | 7.5% |
| Facebook | Email/Phone/Website | 2 | 4 | 2 | 37 | 81 | 568 | 12.48% |
| X | Name/Description | 2 | 7 | 2 | 35 | 89 | 725 | 19.93% |
| **All** | - | 2 | 46 | 2 | 203 | 543 | 10,914 | 4.7% |

## 8 EFFICACY AND ABUSE CONTROL

In this section, we analyze social media accounts that were actioned upon by platforms and evaluate the efficacy of blocking such accounts.

**Detection Overview.** We analyzed the active status of 11,457 social media profiles using API responses from the respective platforms. These responses provided explanations for account actions, such as accounts on *X* being labeled as either *Forbidden* or *Not Found*. The *Forbidden* status indicates that the account was banned due to policy violations, while *Not Found* suggests that the account owner either changed their UserID or voluntarily deleted the account. On *Instagram*, the status appears as *Page Not Found*, while *TikTok*, *YouTube*, and *Facebook* display messages like *Profile/channel does not exist*. We suspect that accounts labeled as *Not Found* or *Does not exist* are likely associated with scammer or abuse profiles. Anecdotally, accounts either go offline intentionally after successfully executing scams or are taken down by the platform for violating policies during the operation of scams. We classify both scenarios under the efficacy of social media platforms in addressing and deactivating such accounts conservatively.

**Findings.** Out of the 11,457 accounts analyzed, the overall efficacy of social media platforms in blocking these accounts was 19.71% (2,259 accounts). A detailed breakdown of inactive accounts and their percentages across platforms is provided in Table 8. Among the five platforms, *TikTok* and *Instagram* demonstrated the highest detection efficacy at 48%, whereas *YouTube* and *Facebook* showed the lowest efficacy at just 5%. Our analysis revealed that blocked accounts frequently featured names associated with trends like *crypto*, *NFTs*, *beauty*, *luxury*, *animals*, or miscellaneous word combinations. This suggests that detection efforts are largely focused on accounts leveraging popular or trending topics. Although *TikTok* and *Instagram* exhibited relatively higher blocking efficacy, given more than 70% of overall visible accounts were created within the last 3.5 years—this period is substantial for scammers to cause significant harm or abuse to online users and platforms. Therefore, while platforms already shown taking proactive detection efforts on these accounts show some promise, the overall efficacy still highlights a concerning gap in addressing and preventing such threats effectively.

**Table 8: Detection Efficacy - In this table we present, the blocking effectiveness of social media platforms that were advertised for sale in open marketplaces. Our observations showed that *TikTok* and *Instagram* had overall 50% of the blocking while *X*, *Facebook*, and *YouTube* blocking lower than 20% of the advertised accounts.**

| Social Media | Visible Accounts | Inactive Accounts | Blocking Efficacy |
|---|---:|---:|---:|
| YouTube | 6,271 | 315 | 5.02 |
| Facebook | 649 | 37 | 5.70 |
| X | 814 | 152 | 18.67 |
| Instagram | 2,023 | 939 | 46.41 |
| TikTok | 1,700 | 816 | 48 |
| **All** | 11,457 | 2,259 | 19.71 |

## 9 RECOMMENDATIONS

Our study shows that accounts that are advertised for selling at these marketplaces undergo preemptive tailoring for future fraud and abuses. Thus the ecosystem of buying and selling social media profiles fosters cybercriminals to operate at scale, making it easy to obtain accounts to launch various cybercrime activities. Throughout these processes, various platforms (e.g., social media, payment vendors) and users are exploited. With that, we would like to provide recommendations for the three parties below.

**Social Media Platforms.** We recommend social media platforms apply stricter and multi-level authenticity that discourages trading of accounts. This includes but is not limited to *(i)* monitoring referral headers that are directed from marketplaces that buy and sell social media profiles, and *(ii)* performing behavioral monitoring of accounts such as rapid follower growth, change of location, or IP addresses that may indicate a likelihood of engagement or account farming. Additionally, we encourage social media platforms to run public awareness campaigns highlighting the risks of account trading, which may involve compromised or illicitly obtained accounts, and to communicate the consequences of platform penalties.

**Payment and Transaction Monitor.** We recommend that payment services such as *PayPal*, *cryptocurrency exchanges*, *wallet providers*, and similar vendors implement robust fraud detection systems to flag transactions linked to the trading of social media accounts. For example, during account verification or onboarding for payment services, a thorough analysis should be conducted to determine the intended use of the service. Similarly, payment platforms should monitor and flag addresses associated with marketplaces facilitating account sales. Establishing strict paywall transaction monitoring and reporting mechanisms would enhance the detection and prevention of fraudulent activities in this context.

**Law Enforcement and Policy Makers.** Currently, the trading of social media profiles operates in a grey area. While social media platforms view such activities as violations of their terms and conditions, such violations result in account bans, which are not explicitly illegal under current laws. This lack of regulation creates a gap in both oversight of social media account trading and consumer protection. We recommend that law enforcement agencies and policymakers explicitly ban the sale of social media profiles by incorporating clear prohibitions in legal frameworks. This is particularly critical as purchased accounts are often misused for malicious purposes. Collaborative efforts with social media companies and *DNS sinkholes* should be enforced to identify and take down domains associated with marketplaces facilitating account sales. Additionally, we propose establishing robust consumer protection measures. This should include penalties for individuals or organizations found engaging in the buying or selling of social media accounts, especially in cases where such practices are likely in the future, use for exploit or defraud others.

## 10 LESSONS LEARNED

In this section, we summarize the main findings of our study and discuss their wider implications.

**The Hidden Scale and Economics of Account Sales.** This paper provides the first large-scale empirical analysis of 38K social media accounts listed for sale, revealing a total market value exceeding \$64M, with median prices differing across platforms (e.g., Instagram: \$298, TikTok: \$755), providing key insights into the economic drivers of this illicit market.

**Old Accounts, New Tricks: Creation Patterns as Fraud Tools.** We provide a novel timeline of account creation, revealing that 30% of sold accounts were created pre-2020, leveraging their longevity to evade detection. Conversely, accounts created in the past 3.5 years still dominate scam activity (~70%), suggesting that scammers quickly adapt to platform changes and user trends.

**Playbooks of Deceit: Fraud Strategies in Marketplaces.** Through analysis of both public and underground marketplaces, we identify coordinated fraud strategies, including high textual similarity (up to 100%) across scam listings, indicating shared playbooks among fraud networks.

**The Anatomy of Scams: Types and Tactics.** We categorize 18.7K scam posts into six distinct types, including financial scams, phishing, and impersonation. This clustering provides actionable insights into how fraudsters operate across platforms. Fraudulent accounts target specific categories (e.g., crypto, gaming, luxury) with tailored narratives to exploit niche communities, demonstrating high levels of operational precision.

**Engagement Metrics Boost Fraudulent Credibility.** By analyzing engagement metrics from 11,457 accounts, we demonstrate how these metrics are exploited to enhance the perceived legitimacy of fraudulent accounts. We observed that accounts are pre-configured with characteristics such as high follower counts and strategic descriptions to enhance their appeal before sale.

**Profiling Seller Activity Across Platforms.** We identify patterns in seller activity, including cross-marketplace operations, and show how sellers replenish listings to align with supply-demand dynamics. Cross-platform activities, including identical seller profiles on the dark web and public marketplaces, highlight a merging of traditionally separate fraud ecosystems.

**Social Media Detection Gaps.** Our results show that, despite platform efforts, only 19.7% of identified fraudulent accounts were actioned upon by social media platforms, underscoring the critical need for enhanced detection methodologies.

## 11 CONCLUDING REMARKS

In conclusion, the rise of online marketplaces for trading social media accounts presents significant risks to platform integrity and user safety. While not inherently illegal, these transactions violate the policies of platforms like X, Instagram, Facebook, TikTok, and YouTube, and fuel fraudulent activities. Our analysis, conducted from February to June 2024, identified 38,253 accounts advertised for sale across 11 marketplaces and 211 distinct categories, representing a total value exceeding $64 million, with a median price of $120 per account. We examined 11,457 visible advertised accounts and collected metadata along with over 200K associated posts. This data revealed fraudulent practices such as bot farming, account harvesting for future scams, and deceptive engagement manipulation. These fraudulent accounts often impersonate legitimate profiles, leveraging social engineering tactics to exploit unsuspecting users. Platforms currently face challenges in detecting and mitigating these threats, leaving users vulnerable to attacks. To address these issues, we provided detailed disclosures to the respective platforms and proposed practical recommendations including indicators to identify and track fraudulent accounts given the scam patterns and tactics we discovered in our research.

## ACKNOWLEDGEMENTS

The authors gratefully acknowledge funding from the German Federal Ministry of Education and Research (BMBF grant 16KIS1900 “UbiTrans”). The authors used GPT-4 and Grammarly to revise the text of most sections to correct typos, grammatical errors, and awkward phrasing.

## REFERENCES

[1] Ares market. https://sn2sfdqay6cxztroslaxa36covrhoowe6a5xug6wlm6ek7nmeiujgvad.link/.

[2] Black pyramid. http://blackpyoc3gbnrlvxqvvytd3kxqj7pd226i2gvfyhysj24ne2snkmnyd.onion/.

[3] Dark matter. http://darkmmro6j5xekpe7jje74maidkkkkw265nngjqxrv4ik7v3aiwdbtad.onion/.

[4] Kerberos market. http://kerberqtg7xpofsc3w47nvjd52sys6hqdejk3h7fz6kbqhyqrds3xgqd.onion/.

[5] Mgm market. https://mgmsanjqxo4svh35yqkxxe5r54z2xc5tjf6r3ichxd3m2rwcgabf44ad.xyz/.

[6] Nexus market. http://nexusabcdkq4pdlubs6wk6ad7pobuupzoomoxi6p7l32ci4vjtb2z7yd.onion/.

[7] Sentence Transformer all-mpnet-base-v2. https://huggingface.co/sentence-transformers/all-mpnet-base-v2.

[8] Torzon market. http://sglgj2fytneccvyn6n4u3pacj4zhdhscfoptnhxxes3uvljmontru2yd.onion/.

[9] We the north. http://hn2paw7zaahbikbejiv6h22zwtijlam65y2c77xj2ypbilm2xs4bnbid.onion/.

[10] Abdelnabi, S., and Fritz, M. {Fact-Saboteurs}: A taxonomy of evidence manipulation attacks against {Fact-Verification} systems. In *USENIX Security* (2023).

[11] Acharya, B., Lazzaro, D., López-Morales, E., Oest, A., Saad, M., Cinà, A. E., Schönherr, L., and Holz, T. The imitation game: Exploring brand impersonation attacks on social media platforms. In *USENIX Security* (2024).

[12] Acharya, B., Saad, M., Cinà, A. E., Schönherr, L., Nguyen, H. D., Oest, A., Vadrevu, P., and Holz, T. Conning the crypto conman: End-to-end analysis of cryptocurrency-based technical support scams. In *IEEE Symposium on Security and Privacy (IEEE S&P)* (2024).

[13] Aggarwal, A., and Kumaraguru, P. What they do in shadows: Twitter underground follower market. In *Annual Conference on Privacy, Security and Trust (PST)* (2015).

[14] Apify. Apify instagram scraper api. https://apify.com/apify/instagram-scraper, 2024.

[15] Apify. Facebook scraper. https://apify.com/streamers/facebook-scraper, 2024.

[16] Apify. Youtube scraper. https://apify.com/streamers/youtube-scraper, 2024.

[17] Bitaab, M., Cho, H., Oest, A., Lyu, Z., Wang, W., Abraham, J., Wang, R., Bao, T., Shoshitaishvili, Y., and Doupé, A. Beyond phish: Toward detecting fraudulent e-commerce websites at scale. In *2023 IEEE Symposium on Security and Privacy (IEEE S&P)* (2023).

[18] Bowyer, G. CLD2-CFFI – Python (CFFI) Bindings for Compact Language Detector 2. https://github.com/GregBowyer/cld2-cff, 2016.

[19] Cao, Q., Yang, X., Yu, J., and Palow, C. Uncovering large groups of active malicious accounts in online social networks. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)* (2014).

[20] Chhabra, S., Aggarwal, A., Benevenuto, F., and Kumaraguru, P. Phi.sh$ocial: the phishing landscape through short urls. In *Electronic Messaging, Anti-Abuse and Spam Conference (EMASC)* (2011).

[21] Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., and Tesconi, M. Fame for sale: Efficient detection of fake twitter followers. *Decision Support Systems* (2015).

[22] DeKoven, L. F., Pottinger, T., Savage, S., Voelker, G. M., and Leontiadis, N. Following their footsteps: Characterizing account automation abuse and defenses. In *ACM SIGCOMM Conference on Internet Measurement Conference (IMC)* (2018).

[23] Egele, M., Stringhini, G., Kruegel, C., and Vigna, G. Compa: Detecting compromised accounts on social networks. In *Network and Distributed System Security (NDSS)* (2013).

[24] Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., and Zhao, B. Y. Detecting and characterizing social spam campaigns. In *ACM SIGCOMM conference on Internet measurement (IMC)* (2010).

[25] Grier, C., Thomas, K., Paxson, V., and Zhang, M. @ spam: the underground on 140 characters or less. In *ACM conference on Computer and communications security (CCS)* (2010).

[26] Grootendorst, M. KeyBERT: Minimal Keyword Extraction with BERT. https://doi.org/10.5281/zenodo.4461265, 2020.

[27] Grootendorst, M. BERTopic: Neural topic modeling with a class-based TF-IDF procedure. *arXiv arXiv:2203.05794* (2022).

[28] IDRC. Social media scams are on the rise as more people use the platforms to connect. https://www.idtheftcenter.org/post/social-media-scams-are-on-the-rise-as-more-people-use-the-platforms-to-connect/, 2020.

[29] Jain, M., Mowar, P., Goel, R., and Vishwakarma, D. K. Clickbait in social media: detection and analysis of the bait. In *Information Sciences and Systems (CISS)* (2021).

[30] Jr., T. H. Social media scams: Stunning statistics and tips to protect yourself. https://www.cnbc.com/2023/10/12/americans-lose-billions-to-social-media-scams-red-flags-to-spot.html, 2023.

[31] Khalil, A., Hajjdiab, H., and Al-Qirim, N. Detecting fake followers in twitter: A machine learning approach. *International Journal of Machine Learning and Computing* (2017).

[32] Li, Z., and Liao, X. Understanding and analyzing appraisal systems in the underground marketplaces. In *Network and Distributed System Security (NDSS)* (2024).

[33] Lin, Z., Cui, J., Liao, X., and Wang, X. Malla: Demystifying real-world large language model integrated malicious services. *arXiv arXiv:2401.03315* (2024).

[34] Lykousas, N., Koutsokostas, V., Casino, F., and Patsakis, C. The cynicism of modern cybercrime: Automating the analysis of surface web marketplaces. In *IEEE International Conference on Service-Oriented System Engineering (SOSE)* (2023).

[35] Maras, M.-H., and Ives, E. R. Deconstructing a form of hybrid investment fraud: Examining 'pig butchering'in the united states. *Journal of Economic Criminology* (2024).

[36] McInnes, L., Healy, J., and Astels, S. HDBSCAN: Hierarchical Density Based Clustering. *Journal of Open Source Software* (2017).

[37] McInnes, L., Healy, J., and Melville, J. UMAP: Uniform Manifold Approximation and Projection for Dimension Reduction. *arXiv arXiv:1802.03426* (2018).

[38] Mehrotra, A., Sarreddy, M., and Singh, S. International conference on contemporary computing and informatics (ic3i). In *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)* (2016).

[39] Milevski, D. Apify telegram scraper api. https://apify.com/danielmilevski9/telegram-channel-scraper, 2024.

[40] Milevski, D. Telemetrio telegram scraper api. https://telemetr.io/, 2024.

[41] Milmo, D. Sharp rise in blackmail of children asked to share explicit images. https://www.theguardian.com/society/2023/may/12/sharp-rise-in-blackmail-of-children-asked-to-share-explicit-images, 2023.

[42] Mirtaheri, M., Abu-El-Haija, S., Morstatter, F., Ver Steeg, G., and Galstyan, A. Identifying and analyzing cryptocurrency manipulations in social media. *IEEE Transactions on Computational Social Systems (IEEE TCSS)* (2021).

[43] Motoyama, M., McCoy, D., Levchenko, K., Savage, S., and Voelker, G. M. An analysis of underground forums. In *ACM SIGCOMM Conference on Internet Measurement Conference (IMC)* (2011).

[44] News, F. Ftc data shows consumers report losing $2.7 billion to social media scams since 2021. https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-data-shows-consumers-report-losing-27-billion-social-media-scams-2021, 2023.

[45] News, F. J'finfluencers' charged for promoting unauthorised trading scheme. https://www.fca.org.uk/news/press-releases/finfluencers-charged-promoting-unauthorised-trading-scheme, 2024.

[46] News, W. P. The rise of sextortion and responses to a growing crime. https://www.weprotect.org/issue/sextortion/.

[47] Popovici, M. Job scams report – 2,670 social media posts reveal scammers top tactics. https://heimdalsecurity.com/blog/job-scam-social-media-study/, 2024.

[48] Puig, A. Fake shipping notification emails and text messages: What you need to know this holiday season. https://consumer.ftc.gov/consumer-alerts/2023/12/fake-shipping-notification-emails-and-text-messages-what-you-need-know-holiday-season, 2023.

[49] Reimers, N., and Gurevych, I. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks. In *Empirical Methods in Natural Language Processing (EMNLP)* (2019).

[50] Ruan, X., Wu, Z., Wang, H., and Jajodia, S. Profiling online social behaviors for compromised account detection. *IEEE Transactions on Information Forensics and Security (ITIFS)* (2016).

[51] Sebastain, N. Social media scams: Stunning statistics and tips to protect yourself. https://www.goodfirms.co/resources/social-media-scams-statistics-and-tips-for-protection, 2024.

[52] Stivala, G., and Pellegrino, G. Deceptive previews: A study of the link preview trustworthiness in social platforms.

[53] Stringhini, G., Egele, M., Kruegel, C., and Vigna, G. Poultry markets: on the underground economy of twitter followers. *ACM SIGCOMM Computer Communication Review* (2012).

[54] Stringhini, G., Kruegel, C., and Vigna, G. Detecting Spammers on Social Networks. In *Annual Computer Security Applications Conference (ACSAC)* (2010).

[55] Stringhini, G., Wang, G., Egele, M., Kruegel, C., Vigna, G., Zheng, H., and Zhao, B. Y. Follow the green: growth and dynamics in twitter follower markets. In *ACM SIGCOMM Conference on Internet Measurement Conference (IMC)* (2013).

[56] SysSec. Buy and Sale of Social Media Code and Data. https://github.com/CISPA-SysSec/social_media_buy_and_sale, 2024.

[57] Thomas, K., McCoy, D., Grier, C., Kolcz, A., and Paxson, V. {Trafficking} fraudulent accounts: The role of the underground market in twitter spam and abuse. In *USENIX Security* (2013).

[58] Trång, D., Johansson, F., and Rosell, M. Evaluating algorithms for detection of compromised social media user accounts. In *2015 Second European Network Intelligence Conference* (2015), European Network Intelligence Conference (ENIC).

[59] Twitter. User detail twitter api. https://developer.twitter.com/en/docs/twitter-api/v1/accounts-and-users/follow-search-get-users/api-reference/get-users-lookup, 2024.

[60] Twitter. User timelines twitter api. https://developer.twitter.com/en/docs/twitter-api/tweets/timelines/introduction, 2024.

[61] Viswanath, B., Bashir, M. A., Crovella, M., Guha, S., Gummadi, K. P., Krishnamurthy, B., and Mislove, A. Towards detecting anomalous user behavior in online social networks. In *Usenix Security* (2014).

[62] Williams, R. The growth of fake products on social media. https://www.redpoints.com/blog/the-growth-of-fake-products-on-social-media/, 2024.

[63] Xiao, C., Freeman, D. M., and Hwa, T. Detecting clusters of fake accounts in online social networks. In *ACM Workshop on Artificial Intelligence and Security (AIS)* (2015).

[64] Xu, T., Goossen, G., Cevahir, H. K., Khodeir, S., Jin, Y., Li, F., Shan, S., Patel, S., Freeman, D., and Pearce, P. Deep entity classification: Abusive account detection for online social networks. In *USENIX Security* (2021).

# A PUBLIC MARKETPLACES PAYMENT METHODS ADDITIONAL DETAILS

In this section, we analyze the supported payment methods by the marketplaces and their security implications.

## A.1 Payment Method Extraction

To identify the payment methods supported by each marketplace, we conducted a comprehensive manual analysis. For each marketplace, we visited its publicly available website and carefully navigated through relevant sections such as payment pages, FAQs, user guides, or checkout interfaces from multiple vantage points, as certain payment methods might only be visible or available to users accessing the platform from specific regions. This ensured that we gathered the most accurate and up-to-date information on payment methods without relying solely on indirect sources like Google search. We recorded all payment methods explicitly listed or implied by the marketplace, such as PayPal, cryptocurrencies, and alternative methods like WeChat Pay and Skrill.

We noted whether the payment methods were visible without requiring user interaction (e.g., creating an account or initiating a purchase). If details were not immediately visible, additional steps such as creating an account were undertaken

**Table 9: Overview of trading channels identified. The table marks all the trading channels monitored in our study, with others not containing account handles publicly or being infeasible to be tracked due to crawling challenges such as CAPTCHAs, complex user interactions, and analysis prerequisites like account credentials.**

| | Exchange | | | Accounts | | |
|---|---|---|---|---|---|---|
| **Category** | **Channel** | **Type** | **Source** | **Selling** | **Handles** | **Monitored** |
| Public | accs-market.com | Marketplace | Google Search | ● | ● | ● |
| | fameswap.com | Marketplace | Google Search | ● | ● | ● |
| | www.z2u.com | Marketplace | Google Search | ● | ● | ● |
| | fameseller.com | Marketplace | Google Search | ● | ● | ● |
| | insta-sale.comlistings/ | Marketplace | Google Search | ● | ● | ● |
| | accsmarket.com | Shop | Google Search | ● | ● | ● |
| | buysocia.com | Shop | Google Search | ● | ● | ● |
| | mid-man.com | Shop | Google Search | ● | ● | ● |
| | socialtradia.com | Shop | Google Search | ● | ● | ● |
| | swapsocials.com | Shop | Google Search | ● | ● | ● |
| | www.surgegram.com | Shop | Google Search | ● | ● | ● |
| | www.toofame.com | Shop | Google Search | ● | ● | ● |
| | cracked.io | Marketplace | [34] | ● | ○ | ● |
| | hackforums.net | BlackHat Forum | Google Search | ● | ○ | ● |
| | swapd.co | Marketplace | Google Search | ● | ○ | ● |
| | accszone.com | Shop | Public BH Forum | ● | ○ | ○ |
| | agedprofiles.com | Shop | Public BH Forum | ● | ○ | ○ |
| | bulkacc.com | Shop | Public BH Forum | ● | ○ | ○ |
| | digitalchaining.mysellix.io | Shop | Public BH Forum | ● | ○ | ○ |
| | discord.gg/PMJCYxCcCu | Shop | Public BH Forum | ● | ○ | ○ |
| | nwarlordyt.sellpass.io | Shop | Public BH Forum | ● | ○ | ○ |
| | famousinfluencer.com | Shop | Public BH Forum | ● | ○ | ○ |
| | nloaccs.com | Shop | Public BH Forum | ● | ○ | ○ |
| | www.smmzone24.com | Shop | Public BH Forum | ● | ○ | ○ |
| | acccluster.com | Shop | Google Search | ● | ○ | ○ |
| | accsmaster.com | Shop | Google Search | ● | ○ | ○ |
| | buyaccs.com | Shop | [57] | ● | ○ | ○ |
| | getbulkaccounts.com | Shop | [57] | ● | ○ | ○ |
| | (bulkye.com) | Shop | [57] | ● | ○ | ○ |
| | quickaccounts.bigcartel.com | Shop | [57] | ● | ○ | ○ |
| | twiends.com | BlackHat Forum | [55] | ○ | ○ | ○ |
| | leakzone.net / | BlackHat Forum | Google Search | ○ | ○ | ○ |
| | magicsmm.com | Shop | Public BH Forum | ○ | ○ | ○ |
| | paneliniz.net | Shop | Public BH Forum | ○ | ○ | ○ |
| | smmorigins.com | Shop | Public BH Forum | ○ | ○ | ○ |
| | smmtake.com | Shop | Public BH Forum | ○ | ○ | ○ |
| | bigfollow.net | Shop | [55] | ○ | ○ | ○ |
| | intertwitter.com | Shop | [55] | ○ | ○ | ○ |
| | seguidores.com.br | Shop | Redirect from bigfollow | ○ | ○ | ○ |
| | scrowise.com | Shop | Google Search | ○ | ○ | ○ |
| Underground | Dark Matter | Marketplace | Onion Directory | ● | ○ | ● |
| | Nexus Market | Marketplace | Onion Directory | ● | ○ | ● |
| | Torzon Market | Marketplace | Onion Directory | ● | ○ | ● |
| | Black Pyramid | Marketplace | Onion Directory | ● | ○ | ● |
| | Kerberos | Marketplace | [33] | ● | ○ | ● |
| | WeTherth | Marketplace | [33] | ● | ○ | ● |
| | MGM Grand | Marketplace | [33] | ● | ○ | ○ |
| | ARES market | Marketplace | Onion Directory | ● | ○ | ○ |
| | Soza | Marketplace | Onion Directory | ○ | ○ | ○ |
| | SuperMarket | Marketplace | Onion Directory | ○ | ○ | ○ |
| | Quantum Market | Marketplace | Onion Directory | ○ | ○ | ○ |
| | Quest Market | Marketplace | Onion Directory | ○ | ○ | ○ |
| | Incognito | Marketplace | Onion Directory | ○ | ○ | ○ |
| | Alias Market | Marketplace | Onion Directory | ○ | ○ | ○ |
| | Archetyp | Marketplace | Onion Directory | ○ | ○ | ○ |
| | City Market | Marketplace | Onion Directory | ○ | ○ | ○ |
| | Elysium | Marketplace | Onion Directory | ○ | ○ | ○ |
| | Fish Market | Marketplace | Onion Directory | ○ | ○ | ○ |
| | Pegasus Market | Marketplace | Onion Directory | ○ | ○ | ○ |
| | Abacus | Marketplace | [33] | ○ | ○ | ○ |
| Contact | Skyisthelimitservice@gmail.com | Email | Public BH Forum | ● | ○ | ○ |
| | t.me/BusinessAts | Telegram | Public BH Forum | ● | ○ | ○ |
| | t.me/sheriff_x | Telegram | Public BH Forum | ● | ○ | ○ |
| | t.me/igexpertbhw | Telegram | Public BH Forum | ● | ○ | ○ |
| | t.me/lulpola | Telegram | Public BH Forum | ● | ○ | ○ |
| | t.me/prudentagency11 | Telegram | Public BH Forum | ● | ○ | ○ |
| | t.me/gunnupgrades | Telegram | Public BH Forum | ● | ○ | ○ |
| | +16193762832 | Whatsapp | Public BH Forum | ● | ○ | ○ |
| | @gunnupg | Discord | Public BH Forum | ● | ○ | ○ |
| | @MaxRuslan369 | Unknown | Public BH Forum | ● | ○ | ○ |

when necessary. To ensure the accuracy of the collected data, we cross-verified each marketplace's payment methods with multiple pages on the marketplace. For platforms with unclear or incomplete information, we performed test interactions, such as attempting to initiate a test transaction, to confirm the availability of specific payment methods.

## A.2 Security Implications

The analysis of supported payment methods across marketplaces reveals a significant variation in availability, reflecting differing priorities in terms of accessibility, user convenience, and security. Table 3 presents the supported payment methods across different marketplaces. Overall, marketplaces that prioritize transparent payment methods and adopt systems with strong buyer protection, such as PayPal and Skrill, provide a safer environment for users. Conversely, reliance on cryptocurrencies or undisclosed payment options increases risks of fraud and dispute resolution challenges.

**Risk of Irreversible Payments.** We observed a wide support for Bitcoin (BTC), Ethereum (ETH), and other cryptocurrencies across marketplaces. While cryptocurrencies enable anonymous transactions, they introduce higher risks due to their irreversible nature and the potential for fraud or illicit activities without buyer protection mechanisms.

**Buyer Protection and Chargebacks.** Digital wallets such as PayPal and Skrill can reduce the exposure of bank card details, and offer users strong buyer protection, including refunds and chargebacks. However, these payment methods are adopted only by two marketplaces (Z2U and FameSeller).

**Regional Payment Methods and Vouchers.** NeoSurf and Payssion, supported by select marketplaces like Z2U, cater to regional or prepaid needs, providing alternatives to bank-linked systems. These methods enhance user privacy by not linking transactions to bank accounts or personal information but offer limited recourse in disputes or fraud cases.

**Escrow-Like Systems.** Trustap and Payer, available on MidMan and TooFame, enhance security by holding funds in escrow until predefined conditions are met, reducing fraud risks for high-value or deferred-delivery transactions. However, their effectiveness depends on the trustworthiness and terms of the escrow provider.

**Transparency of Payment Methods.** For marketplaces such as Accsmarket, FameSwap, and TooFame, payment methods were *unknown* or not publicly disclosed, increasing the likelihood of users interacting with unprotected or insecure systems.