An Explorative Study of *Pig Butchering* Scams

Bhupendra Acharya
CISPA Helmholtz for Information Security
bhupendra.acharya@cispa.de

Thorsten Holz
CISPA Helmholtz for Information Security
holz@cispa.de

***Abstract*—In the recent past, so-called *pig-butchering* scams are on the rise. This term is based on a translation of the Chinese term *Sha Zhu Pan*, where scammers refer to victims as *pig* which are to be "fattened up before slaughter" so that scammer can siphon off as much monetary value as possible. In this type of scam, attackers perform social engineering tricks on victims over an extended period of time to build credibility or relationships, in contrast to similar scams such as romance, cryptocurrency, investment, and job fraud. After a certain period, when victims eventually transfer larger amounts of money to scammers, the fraudsters' platforms or profiles go permanently offline and the victims' money is lost.**

In this work, we provide the first comprehensive study of pig-butchering scams from multiple vantage points. Our study analyzes the direct victims' narratives shared on multiple social media platforms, public abuse report databases, and case studies from news outlets. Between March 2024 to October 2024, we collected data related to pig butchering scams from (i) four social media platforms comprised of more than 430,000 social media accounts and 770,000 posts; (ii) more than 3,200 public abuse reports narratives, and (iii) about 1,000 news articles. Through automated and qualitative evaluation, we provide an evaluation of victims of pig-butchering scams, finding 146 social media scammed users, 2,570 abuse reports narratives, and 50 case studies of 834 souls from news outlets. In total, we approximated losses of over $521 million related to such scams. To complement this analysis, we performed a survey on crowdsourcing platforms with 584 users to broaden the insights on comparative analysis of pig-butchering scams with other types of scams. Our research highlights that these attacks are sophisticated and often require multiple entities, including policymakers and law enforcement, to work together alongside user education to create a proactive detection of such scams.

1. Introduction

According to the Federal Bureau of Investigation (FBI), in 2022, investment-related fraud resulted in $3.31 billion in losses [1], [2]. In 2023, this type of fraud accounted for $4.57 billion, an increase of 38% over the previous year [3]. In 2024 alone, the FBI received 18K complaints, reporting $1.9 billion losses [4]. These loss metrics are only accounted from reported ones and many go unreported as victims do not report being scammed due to several psychological, emotional, and social factors [5], [6], [7].

In recent years, a specific type of investment-related fraud became prominent: the phenomenon of *pig-butchering* scams has emerged as a significant threat in the landscape of social engineering [8], [9], [10], [11]. The term *pig-butchering* is derived from the Chinese phrase *Sha Zhu Pan*, where fraudsters establish trust with a victim through romance or a similar trustworthy relationship, metaphorically "fattening the pig" before conning them [12]. Fraudsters later deceive the potential victim into investing via a fake investment platform or asking for a transfer of funds making a fake emergency support before finally "butchering" them. Overall, pig-butchering scams are a more recent and sophisticated evolution of romance [13], [14] and investment scams [15], [16], where fraudsters exploit the popularity and complexity of cryptocurrency to deceive victims. These scams involve emotional manipulation or promises of quick, low-risk returns through fraudulent investments.

Pig-butchering scams typically begin with fraudsters reaching out to potential victims through social media [17], [18], [19], dating apps [20], [21], [22], or other online platforms [23], [24]. Such scams are often orchestrated by gangs of scammers, or by abducted and trafficked humans who are forced to perform scams on target their victims, establishing relationships that last weeks to months [25], [26]. In a fraudulent investment scenario, the victim receives some profitable returns upon investing and can withdraw, which builds the credibility of the investment whereas for romance fraud, the victim is asked to support the fraudsters in emergency financial support before the victim, and fraudsters can physically meet. In both cases, when the victim either increases their transfers or investments to larger amounts or can no longer transfer or invest, the fraudulent investment platforms block withdrawals, citing fake technical issues, or they go offline altogether. In romance scams, messaging apps, social media, or dating profiles eventually go offline as well, leaving the victim defrauded [27].

Although the security community has recently begun exploring pig-butchering scams via technical reports [28], [29], [30], [31], and academic papers [32], [33], [34], [35], [36], [37], [38], there is still a lack of detailed understanding of how fraudsters set up social media profiles and engage with victims using various social engineering techniques as part of the scam orchestration. While the prior research has examined various aspects of financial fraud and cybercrime, including phishing, identity theft, and investment fraud, the specific phenomenon of pig-butchering scams remains under-explored. Existing literature often focuses on the economic impact of such crimes and general strategies for prevention and detection [39], [40], [41], whereas exploration of scammer engagement including multiple social media platforms and channels of communication was not studied yet.

In this paper, we systematically study fraudsters carrying out pig-butchering scams from three sources: (i) social media platforms such as *X* (formerly known as Twitter), *Instagram*, *Telegram*, and *YouTube*, (ii) public reported abuse databases such as *Chainabuse* [42], and *Crypto Scam Tracker* [43], and (iii) news articles case studies on pig-butchering scams. Through these three vantage points, we collect the victim's direct or attempted pig-butchering experiences and provide a detailed analysis of the scam life cycle. Additionally, we perform quantitative studies through crowd-sourced surveys to further add detail to online scams and fraudsters' strategies.

More specifically, we performed the first large-scale study of pig-butchering via (i) multiple social media platforms, collecting 431,731 social media accounts and 771,245 posts, with 146 confirmed victims of pig-butchering scams; (ii) collecting 3,213 narratives related to abuse report on public database with 2,570 confirmed narratives of being a victim of pig-butchering scams; (iii) collecting 1,074 news outlets, through automated and qualitative analysis confirming 50 unique case studies related to 834 victims of pig-butchering. We performed tracking and evaluation of scam mechanics including scammer's fraudulent channels and payment method. Through this study, we approximated the total loss from victims (146 social media users, 2,570 abuse databases narratives, and 50 case studies of 834 souls) collectively losing over $521 million tied to pig-butchering scams. Additionally, we performed a quantitative study via a crowd-source platform with 586 participants to broader understand the online scams experience of in-the-wild users, and provide a comparative analysis with pig-butchering scams. Finally, we provide recommendations to better defend against such scams in the future.

We summarize our key contributions as follows:

- **Large Scale Study on Pig-butchering Scam.** We present the first large-scale study on pig-butchering scams across three sources: social media platforms, abuse-reported databases, and new articles on first-hand reports of experiences with fraudsters operating globally. Additionally, we perform user studies (n=586) via a survey to provide further insights on online scams in comparison to pig-butchering scams.
- **Scam Mechanics and Fraud Tracking.** We provide a comprehensive analysis of the modus operandi of scammers executing pig-butchering schemes, identifying their fraudulent schemes and the payment methods they use as part of these scams. Our research provides an in-depth analysis of fraudsters' life cycle operations that are orchestrated via various platforms.

To foster research, we share our code [44] and data related to victim's experiences. However, for data protection reasons, the data related to identifying scammers (e.g., social media profiles, emails, URLs, and cryptocurrency addresses) are only shared with interested academics, abused entities, or researchers upon request.

2. Related Work

To the best of our knowledge, this work is the first large-scale, systematic study to conduct a comprehensive analysis of pig-butchering scams using several data sources. Below, we discuss relevant prior studies, highlight the unique aspects of our research, and address the existing research gap.

Cryptocurrency, Investment, and Romance Scams. Previous studies have investigated various types of abuse and scams in cryptocurrency [45], [46], [47], [48], investment [49], [50], [51], and romance domains [52], [53], [54], [55]. For instance, Bartoletti et al. [45] examined the prevalence of cryptocurrency scams and developed a taxonomy of the types of attacks used by cryptocurrency fraudsters. Xia et al. [46] focused on cryptocurrency scams that emerged during the COVID-19 pandemic. In the area of romance fraud, Buchanan et al. [52] and Whitty et al. [53] analyzed online romance scams where fraudsters target potential victims by pretending to seek an intimate relationship. However, none of the previous studies performed a comprehensive end-to-end tracking of cryptocurrency and the life-cycle of pit-butchering scams in comparable contexts.

Pig-butchering Scams. Although pig-butchering scams are relatively recent, researchers from various fields have begun examining the abuse [56], [57], [58] and its impact on victims [32], [33], [37]. For example, Wang [32] describes the experiences of trafficked Chinese workers who are forced into pig-butchering scams. Burton et al. [56] provides an overview of the methodologies behind these scams through a literature review survey, and Cross et al. [57] analyze the evolution of social engineering tactics used by fraudsters in romance and cryptocurrency scams. The close work from ours by Maras et al. [58] focuses on investment fraud, analyzing news articles and court documents with an emphasis on criminal justice practices.

Abuse study on Social Media Platforms. Over the past five years, social media has become a key platform for studying scams and abuses across various topics, including cryptocurrency scams [59], [60], brand and user attacks [61], [62], hate speech [63], [64], [65], and psychological abuse [66], [67]. With *HoneyTweet* [59], Acharya et al. examined fake technical support scams targeting popular cryptocurrency wallet users, while Ratkiewicz et al. [68] investigated the tracking and detection of political abuses propagated through social media. Despite these efforts, a research gap remains in identifying first-hand victims involving online platforms in pig-butchering scams.

Study on Public Abuse Reports. Previous studies on public abuse reports have examined various aspects of cryptocurrency-related abuse, such as categorizing types of cryptocurrency abuse [69], [70], [71], tracking abuse campaigns on the dark web [72], [73], and analyzing infrastructure models in abuse reports [74], [75]. However, no prior research has focused specifically on abuse reports of victims of pig-butchering scams.

3. Evaluation Setup and Methodology

In this section, we present our evaluation setup and methodology to understand the life cycle of a pig-butchering scam. Our system is composed of three main modules, as illustrated in Figure 1: ❶ gathers data from three sources: (i) social media platforms, (ii) publicly reported abuse incidents related to pig-butchering scams, and (iii) news articles related to pig-butchering scams collected from multiple search engines; ❷ performs semi-automated filtration on such collected data to ensure the data are related to this kind of scams; ❸ performs the quantitative study on users experiencing online scams in the last five years recruiting through a crowd-sourced platform, and ❹ analyzes the aggregated data collected to further validating the fraudulent activities via tracking scamming profiles and abusing payment methods. We provide descriptions of our approach below and discuss ethical considerations and the disclosure process in Appendix 9.

3.1. Search Methodology and Raw Dataset

From March 2024 to August 2024, we collected data from three primary sources: (i) social media platforms, (ii) public reports submitted to cryptocurrency abuse databases, and (iii) news articles about pig-butchering scams. For organizing relevant data searches on social media, we manually crafted keywords based on observations of public posts across various platforms. For abuse reports and news articles, we focused keyword searches on the terms “pig-butchering”, “romance scam”, and “investment scam”. Below, we provide further details on our search methodology and raw data collection process. We discuss the potential limitations of the data sets in Appendix 9.

3.1.1. Manual Search Keywords Collection. During our research incubation period, we performed a manual search on multiple social media platforms to identify cases and abusive profiles related to pig-butchering. From our observations, we identify three categories of pig-butchering schemes targeted to individuals looking for an *online dating/romance*, *investment*, and *job*. We observe first-hand victims mentioning these stories throughout their posts. We take these three schemes as ground truth for the formation of keywords in social media posts to search for relevant pig-butchering posts. Based on our manual observation, we created a total of 219 keywords that we used as part of search posts on social media platforms. In Appendix A, we provide further detail on this keyword-gathering methodology. For abuse databases, we focused our data search on the scam tag classification provided by abuse databases from *Chainabuse* and *Crypto Scam Tracker*. In reviewing these databases, we found that numerous complaints were categorized as pig-butchering scams, investment fraud, or romance scams. We included investment fraud and romance scams in our analysis because pig-butchering scams often involve advanced social engineering tactics, where victims are groomed over a prolonged period. As a result, we focused our analysis on reports marked with these classifications.

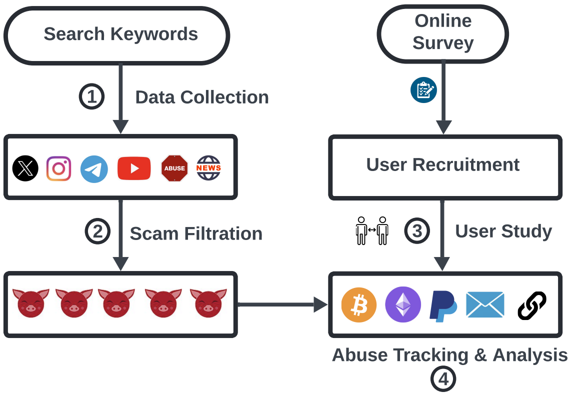


Figure 1: Data Collection – Our system comprises three main modules. Based on our manual observations of direct victims of pig-butchering scams, we developed search keywords to collect data from various sources (❶). After collecting the data, we apply automated and manual filtration of data (❷). Additionally, we perform quantitative studies via survey on online scams (❸), and finally, we evaluate the collected data by tracking and profiling abusive elements and victims’ narratives (❹).

3.1.2. Semi-Automated Data Collection. We collected data from social media platforms by performing automated API calls using search keywords, while data from abuse databases was gathered through a combination of collaboration and manual downloads. We provide details on each source below.

Social Media Data. We perform keyword-based searches on four social media platforms: *X*, *Instagram*, *Facebook*, and *Telegram*. In particular, we automated API services [76], [77], [78], [79], [80], [81] to collect the data from these social media platforms. We provide a breakdown of the raw dataset from each of these social media in Table 1. In total, we collected 789,751 posts from 432,762 users from these platforms. For each of the social media users, we further collected the profile metadata such as profile name, descriptions, location, followers, and profile image. Among this platform, *X* comprised the highest number of posts and accounts—overall 53% (414,992/771,245) of the posts comprised 76% (328,822/431,731) of accounts stored in our database. The lowest count resulted from *YouTube*, 21% (93,618/431,731) accounts comprised of 9% (71,607/771,245) posts. Our dataset from all four social media platforms had a median of 49,182 accounts and 142,323 posts.

Table 1: Overview of the raw dataset obtained by performing search queries across four social media platforms. Among the four social media platforms, we observe that *X* contains the largest number of accounts and posts.

Platform	Accounts	Distinct Posts	All Posts
X	328,822	125,264	414,992
Instagram	4,746	175,000	190,236
Telegram	4,545	94,410	94,410
YouTube	93,618	65,295	71,607
All	431,731	459,969,	771,245

Table 2: Overview of the raw dataset on news articles related to pig-butchering scams obtained by performing search queries across three search engines via web search and news search methodology. Among the three search engines, we observe that *Bing* contains the largest number of articles.

Search Engines	Web Search	News	All Articles
Yahoo	167	110	172
Google	157	355	477
Bing	237	466	682
All (Distinct)	355	871	1074

Public User Reported Data. We collected public user reports on pig-butchering scams, particularly those involving narratives tagged with pig-butchering scams. We collaborated with *Chainabuse*, a well-known cryptocurrency abuse reporting platform, for fetching the data associated with public reports on pig-butchering. The second data source was manually downloaded from *Crypto Scam Tracker*, Department of Financial Protection and Innovation, Official website of the State of California. In Table 3, we provide a summary of the public reports gathered from both sources. In total, we collected 3,213 public narratives associated with 1,710 distinct complaints.

Public News Articles. We collected publicly available news articles on pig-butchering scams using a custom Python Selenium automation. For this process, we utilized three search engines: *Google*, *Bing*, and *Yahoo*. Our choice of these search engines is motivated by their popularity [82]. For each search engine, we automated searches across their *web search* and *news search* features using the keyword *pig-butchering scam*. For the search limits, we restricted the web search to the first 30 pages, while the news search was limited to the maximum scroll permitted by each search engine on its news page. As summarized in Table 2, we collected a total of 1,074 news articles from these sources, with *Yahoo* contributing the fewest at 16% (172/1,074) and *Bing* the most at 63% (682/1,074).

Table 3: Overview of the abuse database: In this table, we highlight pig-butchering scam complaints gathered from two public sources. These public reports include victim complaints about close encounters with scammers, along with narrative details describing their interactions.

Abuse DB	Reports	Narratives
Chainabuse	1,467	2,970
Crypto Scam Tracker	243	243
Total	1,710	3,213

3.2. Data Filtration and Candidate Selection

We applied three distinct data filtration processes to the collected data. First, for social media platforms, we used prompt queries backed by large language models (LLMs) to identify posts from direct victims of pig-butchering scams. Second, for public reports, we ensured that each report was consistently tagged by users as a pig-butchering scam complaint and conducted manual reviews of each narrative. Lastly, for news articles, we filtered out irrelevant articles and performed a thorough qualitative review. We provide additional details on each of these sources as below.

3.2.1. Data Filtration on Social Media. To identify victims of pig-butchering scams, we initially applied two automated methods: (i) keyword heuristics to assess post engagement, specifically targeting users who mentioned being scammed by referencing terms like *scam*, *fraud*, and *lost*, along with first-person pronouns (*I*, *me*, and *my*); and (ii) prompt engineering with large language models (LLMs) to detect content related to specific fraudulent activities, including pig-butchering, romance scams, investment scams, and cryptocurrency scams. Through these automated approaches, we identified 0.27% (2,096/771,245) of distinct user narratives as potential scam reports from the overall raw dataset, sharing 123 narratives from both automated techniques: LLMs, and keyword heuristics. Acknowledging prior work that LLMs can produce hallucinations [83], and Natural Language Processing (NLP) heuristics could contain inaccurate content filtering [84], we then conducted a manual dataset evaluation of these posts across four social media platforms, confirming 146 accounts sharing their personal experience of pig-butchering scams. During the manual review, we ensured that identified pig-butchering cases involved extended grooming periods, distinguishing them from standard romance and investment scams. In Table 4, we present a breakdown of filtered victims by social media platform and methodology, with additional details on prompt-engineering filtration available in the Appendix B.

3.2.2. Data Filtration on AbuseDB. We conducted a manual review of 3,213 narratives from 1,710 posts to ensure our collected data accurately represented cases specific to pig-butchering scams. In our manual review, we classified narratives based on two scenarios: (i) cases tagged as pig-butchering that contained narratives clearly showing characteristics of pig-butchering scams, and (ii) cases tagged under related categories, such as romance and investment fraud, that involved prolonged victim grooming were reclassified as pig-butchering. We included specifically romance and investment fraud cases because pig-butchering scams are

Table 4: Overview of social media-based victim filtration from the raw dataset applying automated (LLMs, and NLP-heuristics) and manual reviews. Between the two filtration methods, we found that LLM-based filtering identified more victims than NLP-based heuristics. Additionally, *YouTube* had the highest number of users willing to openly share their experiences as victims compared to other social media platforms.

Platform	LLMs	NLP-Heuristics	Manual Reviews
Instagram	2/84	7/372	9
Telegram	10/228	2/151	12
X	5/69	29/321	34
YouTube	68/221	23/835	91
All	85/602	61/1679	146

often structured around similar tactics of prolonged victim grooming. During this review, we filtered out duplicated reports, narratives related to other types of crypto scams (such as sextortion or blackmail), and entries with insufficient information to confirm relevance to pig-butchering scams. Through this filtering process, we excluded 13% (232/1,710) of the reports and 19% (642/3,213) of the narratives. As a result, our final dataset of abuse reports includes 1,478 unique reports comprising 2,570 narratives.

3.2.3. Data Filtration on News Articles. Our news filtration process involves several semi-automated steps. First, we filtered out 97 URLs linked to unrelated content, such as *YouTube* videos and social media posts from *X* or *Instagram* about pig-butchering. For the remaining 977 URLs, we performed a Python URL alive check to confirm active links, retaining only those with response codes between 200 and 300. This process filtered out an additional 19 inaccessible URLs. To ensure the content was relevant to pig-butchering, we developed a custom Selenium Python script to retrieve page content, identifying 410 URLs containing pig-butchering context. Recognizing that some automated page visits are blocked, we checked for *CAPTCHA* terms to be present on the page source content, identifying 92 URLs restricted by *CAPTCHA*. From the multiple stages of filtration, we selected 501 URLs as candidate links and performed a qualitative manual review of them.

3.3. User Study

Our third module conducts a representative quantitative study on users' experiences with online scams over the past five years. For this study, we recruited survey participants from crowd-sourcing platforms to assess the frequency of online scams and identify which types are most common, including classic scams such as phishing, technical support fraud, online shopping scams, and identity theft. Additionally, we provide a comparative analysis of users' experiences with pig-butchering scams. Through this study, our aim was to gain a deeper understanding of victim experiences, particularly with pig-butchering scams, and to provide broader insights into various other types of scams.

3.4. Tracking and Analysis

The fourth module, *abuse tracking and analysis*, offers insights into scammer engagement, along with quantitative analysis of victim losses, impacts, and the methods fraudsters use to lure victims. This module performs an in-depth analysis of various elements associated with both pig-butchering scams and their victims. It includes features such as engaged posts, victim narratives, scam-related social media profiles, linked payment methods cryptocurrency addresses, and operational techniques used throughout the scam's life-cycle.

Paper Outline. For the rest of the section organization, we present our findings as follows: social media abuse measurement in Section 4; public reported abuse reports evaluation in Section 5; evaluation of new media and coverage on victims of pig-butchering in Section 6; tracking fraudulent communication channels, external URLs, and payment methods of scammers in Section 7; representative quantitative users study experiencing online scams in Section 8 and ethical consideration and data limitations in Section 9. Summarizing our findings, and insights collected from the victim's experiences, we provide the recommendations in tackling pig-butchering scams in Section 10.

4. Social Media Abuse Measurement

In this section, we provide the qualitative analysis of 146 pig-butchering victims found on social media, focusing on three key areas: (i) confirmation of financial losses, (ii) the scammer's methods and tactics used in the operation, and (iii) the victim's post-scam experiences, including the impact on their lives as described in their public posts.

Overview. In Table 5, we show the total reported losses by victims on each social media platform. Of the four platforms, victims on *YouTube* reported the highest total loss, with $14,341,820 from 58/91 victims, while *Instagram* showed the lowest reported loss of $2,200 from 2/9 victims. Our analysis reveals that 57% (84/146) of victims openly disclosed their financial losses due to scams. Additionally, 65% (95/146) of victims shared details on the specific social engineering techniques used by scammers. We identified eight distinct scamming tactics: Crypto Schemes (41/146), Romance scams involving financial transfers (21/146), Investment/Impersonation (10/146), Romance scams with false crypto investment promises (9/146), Fake Job offers (8/146), Bogus Seller Business Setup (2/146), Romance scams leading to online coercion (2/146), and Romance scams resulting in Identity Theft (2/146). In Figure 2, we illustrate the breakdown of these scam techniques based on victim reports on each social media platform. We provide additional details on each social media platform below.

Table 5: Approximated Dollar amount losses from the disclosed victim from social media dataset - This table provides an estimated dollar value for losses reported by victims. It includes the lower-bound approximated financial losses, with international currencies and cryptocurrencies converted to USD based on exchange rates and cryptocurrency values from the first week of November 2024.

Platform	Disclosed	All Victims	Approx. Amount
Instagram	2	9	$2,200
Telegram	6	12	$371,538
X	18	34	$426,745
YouTube	58	91	$14,341,820
All	84	146	$15,142,303

4.1. Evaluation on Instagram

Among the four social media platforms, we identified 6% (9/146), the lost number of victims sharing their experiences that relate to pig-butchering scams. We provide further details below.

Victim Confirmation and Financial Looses. As Instagram is widely used for sharing photos and videos, we suspect that victims are reluctant to share posts compared to other social media platforms. Among the 9 victims' experiences, only two victims shared their experience of losing between $200 – $2000 in package delivery scams, where fraudsters lured victims into investing in "unclaimed package" boxes and such boxes never arrived to victims.

Scam Tactics. We identified four distinct natures of scam tactics as part of a shared experience of being scammed. These include (i) 4/9 fraudulent crypto schemes (e.g., *OneCoin*, *EXW Wallet*), (i) 4/9 romance scams involving financial requests (iii) 2/9 bogus seller scams (e.g., premium Netflix accounts, unclaimed package sales), and (iv) 1/9 in-person impersonation scams scammer posing as official personnel, visiting victim in person with counterfeit ID.

Victim's Emotional Experience. Out of the nine victims, two reported receiving a ring from a scammer, only to later realize it was a scam. Another two victims filed multiple complaints with the Better Business Bureau regarding the unclaimed package investment scheme, expressing frustration that their complaints were ignored, resulting in unresolved financial losses.

4.2. Evaluation on Telegram

Victims on Telegram account for 8% (12/146) of our overall dataset, making it the second-lowest platform by victim count, following Instagram. Our evaluation of victims' narratives on Telegram is summarized below.

Victim Confirmation and Financial Losses. Of the 12 victims identified on Telegram, 6 victims disclosed their financial losses, while 6 did not reveal the amount lost. Among those who reported their losses, 3 victims collectively lost a total of 110 ETH, with individual losses of 10 ETH, 40 ETH, and 60 ETH. Additionally, two victims reported losing 425 INR, 175 INR, and 250 INR, respectively. The remaining victim lost 5M $BLV tokens, although the exact value of the loss is unclear. The total amount approximated to $371,538 based on the currency conversation rate of the first week of November 2024.

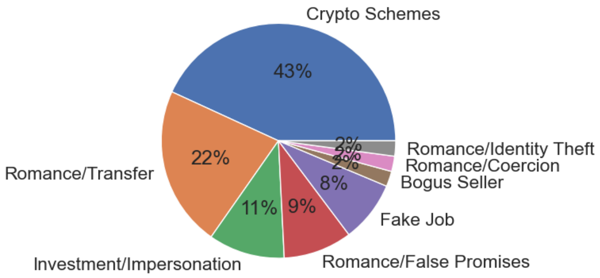


Figure 2: Scam Techniques in Victim Reports on Social Media Platforms - The graph presents eight scam techniques used by scammers in social engineering tactics associated with pig-butchering scams. Our findings indicate that *Crypto Schemes* are the most prevalent, accounting for 43% of all victim reports, while Romance scams involving *Identity* and *Coercion* are among the least reported.

Scam Tactics. We identified three distinct types of scam tactics related to employment and investment scams. These include: (i) 7/12 victims experienced stolen funds and tools, where several victims reported losing large amounts of cryptocurrency, often during private sales or pre-sale events, which they later discovered to be fraudulent; (ii) 3/12 victims were affected by escrow-related fraud, where a deal was arranged through an escrow system, the victim agreed to work, but the scammer failed to make payment; and (iii) 2/12 victims were misled by false promises of refunds or future compensation, with scammers assuring refunds once liquidity pools were unlocked.

Victim's Emotional Experience. We observe three main emotional experiences shared by 9/12 victims. These include (i) (4/9) messages warning others about specific scammer naming them and their experiences to public Telegram forums, (ii) (2/9) acceptance and moving, reflecting on the loss with a degree of acceptance, stating that it's better to recover something rather than nothing. These individuals also emphasize the importance of moving forward and not dwelling on the scam, and (iii) (3/9) emotions like anger, frustration, and even suicidal thoughts are mentioned, where one of the victims shared mentions, "Before I die, I will make sure I kill this scammer" an indication of the serious emotional toll these scams take on victims.

4.3. Evaluation on X

While *X* platform had the highest number of posts and accounts in our raw dataset, it ranks second in reported victim count, representing 23% (34/146) of the total. Below, we provide victims' shared experiences and highlight the details collected from our analysis.

Victim Confirmation and Financial Looses. Out of 34 individuals, 32 individuals shared their victim's experience with confirmed financial losses, while 2 narrowly avoided being scammed by growing suspicious during their interaction. Of the 32 confirmed victims, 14 shared their emotional experiences without specifying their actual financial losses, while 18 reported both the emotional impact and the amount lost. Among those who disclosed amounts, losses ranged from over $250,000—the highest reported, tied to a life-saving investment fraud—down to $200, which was requested under the pretext of a romantic gesture. The median loss among victims was $2,500. From these, two reported their losses in Ethereum, and two in Euros. We approximated the dollar values for Ethereum and Euros. In total, we approximated, $426,745 based on the conversion rates of the first week of November 2024.

Grooming Period. Regarding the duration of grooming, 21 cases did not specify a timeline, 9 described scams occurring within a short span (1-6 weeks), and 7 mentioned prolonged periods exceeding 7 weeks. One case reported a scam that lasted over three years as an intermittent relationship.

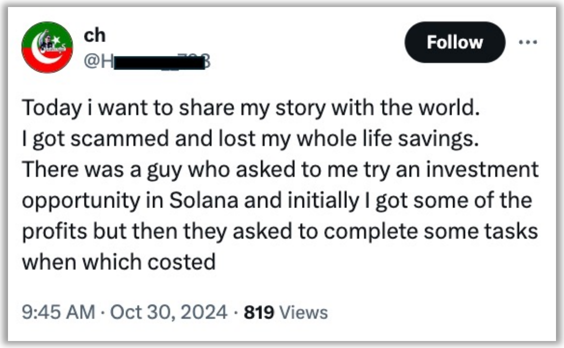
Scam Tactics. We identified 25/34 victims who reported scammer's tactics as part of being scammed. These include romance scams with false promises (9 cases), investment fraud through fake tokens (4) (see Figure 3), high-profile impersonation in investment fraud (4), celebrity impersonation in romantic schemes (4), online coercion in romantic scams (2), and identity theft in romance scams (2).

Victim's Emotional Experience. We observe that 20/25 victims' narratives share their feelings of shame, self-blame, and distrust following scams, showing that these scams impact mental health as well as finances. Examples of shared emotional impacts include (i) (6/25) the victim's accounts being blocked, left in emotional distress, (ii) (4/25) the victim being left with debt, unaware until receiving a default notice or bills, (iii) (3/25) led to life-altering decisions, (iv) (3/25) victim feels devastated, looking for community support, (v) (2/25) victim suffered emotional trauma, blames self, leads to lasting shame, and (vi) (2/25) perpetrator used victim's photos to scam others, leading to guilt or shocked.

4.4. Evaluation YouTube

Across the four social media platforms, we identified 62% (91/146) of the total shared victim experiences, the highest proportion among them. We present our findings in four key areas, with insights detailed below.

Victim Confirmation and Financial Looses. For YouTube, we relied on YouTube's description part of the YouTube channel in gaining the experience shared by the victim. We only included descriptions that provided the direct experience related to the individuals rather than a generic channel of pig-butchering. Out of 91 victims' experiences, we identified three different confirmations: (i) 82/91 channels featured on behalf of victims sharing their losses, and emotional experiences, (ii) 5/91 self-featured channels by victims, and (iii) 4/91 shared nearly being scammed by scammer, and raising awareness throughout the video sharing their tips on the ongoing the pig-butchering scams. Among the nationality-shared information, we identified 58/91 victims from 7 different nationals: US (27), Singapore (9), United Kingdom (8), India (6), Canada (4), New Zealand (2), and Australia (2). The loss amount reported total from eight currencies: USD (4,419,000), SGD (99,000), EUR (3,977,100), GBP (3,314,250), INR (362,358,000), CAD (500,000), AUD (850,000) and JPY (574,470,000), totaling to $14,341,820 based on the currency conversion rate of fist week of November 2024.



ch
@H[redacted]

Today i want to share my story with the world.
I got scammed and lost my whole life savings.
There was a guy who asked to me try an investment opportunity in Solana and initially I got some of the profits but then they asked to complete some tasks when which costed

9:45 AM · Oct 30, 2024 · **819** Views

Figure 3: In this figure, we display *X* posts from a user describing the experience of a fraudulent cryptocurrency investment-based pig-butchering scam. The victim shares an experience of being scammed to raise awareness about fraudulent investment schemes.

Grooming Period. Our analysis of victim reports revealed varying grooming periods based on the type and complexity of scams: (i) cryptocurrency investment scams typically lasted 3-8 weeks, (ii) romance scams involving a relationship spaned 4 weeks to 6 months, (iii) romance scams with an investment took 2-4 months, (iv) romance scams with fake celebrities were discovered by victims with suspicious behavior within hours to days, and (v) long-term manipulation in romance scams, where scammers repeatedly extract money, reported to last several months to a year. These cases highlight that pig-butchering scams involving financial manipulation, especially romance scams, scammers engage in longer grooming to build trust with victims to facilitate significant financial transactions.

Scam Tactics. From the shared experience, we observed scammers performing various social engineering tricks on users: (i) 24/91 victims resulted in high-value losses from $100K to over $1Mil from fraudulent cryptocurrency investment, (ii) 17/91 includes cases like fake romantic partners asking for money, (iii) 5/91 scammers performing impersonation with fake identity use posing as military, doctors, or wealthy investors, and 3/91 scammer performed job fraud / fake opportunities that result in money losses.

Victim's Emotional Experience. We observe 38/91 victims' complex emotional experiences being shared, often affecting multiple aspects of their lives and relationships. These include: (i) the victim felt a sense of betrayal after deeply getting connected with the scammer (12/91), (ii) faced significant losses leading to despair over life's savings (8/91), (iii) life after the scam impacted the family dynamics and relationship (5/91), (iv) anxious and fearful about financial security and suicidal thoughts (4/91), (v) anger and frustration at the difficult to recover (3/91), (vi) embarrassed to share and self low esteem (3/91), (vii) despite the trauma, 3/19 victims felt need to share their stories to the media.

5. Public Abuse Reports Evaluation

In this section, we present an evaluation of 2,570 victim narratives gathered from two sources: *Chainabuse* and *Crypto Scam Tracker*. Our analysis focuses on five key categories: (i) the initial contact method used by scammers, (ii) how scammers build relationships with victims, (iii) the techniques scammers employ to steal funds, (iv) emotional and psychological manipulation, and (v) the financial and psychological impact on victims. We provide our data evaluation techniques and findings as follows.

5.1. Technical Setup and Filtration

We conducted both automated and manual checks on 2,570 narratives. We provide detail on automated checks, and filtration as below.

Heuristics Categorical Filtration. In heuristics-based categorical filtration we created keywords based on random 250 narrative observations in each category. To identify the initial contact method, we applied regex searches for keywords such as *contact*, *app*, or specific social media platform names such as *Twitter*, *Instagram*, *WhatsApp* and others. For relationship-building tactics, we looked for keywords indicating *photo* sharing, *screenshots*, *attachment*, or romance-related words (e.g., *love*, *charm*, *beautiful*, *handsome* as well as investment terms (e.g., *fast*, *return*, *easy*, *crypto*). To detect scammers' techniques for stealing funds, we searched for indicators of payment methods like *PayPal*, *bank*, *credit card*, *cryptocurrency addresses*, *email*, *URL*, and *phone*. In the categories of emotional and psychological manipulation, we focused on expressions of urgency, false promises, and guarantees. For financial and psychological impacts, we perform searches for keywords such as *loss*, *savings*, *bankruptcy*, *depression*, *anxiety*, *betrayal*, *shame*, and *guilt* which reflect victims' financial losses and mental health impacts.

Sub-Categorical and Quantitative Filtration. For three categories—*Relationship-Building*, *Scammer Techniques*, and *Financial and Psychological Impact*—we developed LLM-based prompt queries to identify further sub-categories [85]. This included prompts to explore specific relationship-building techniques used by scammers, the scamming tactics applied to victims, and the financial and psychological impacts victims face post-scam. For *Initial Contact* and *Financial Loss Metrics*, we used keyword-based extraction to identify associated values instead of prompt-based querying.

Manual Quality Check. In addition to the two automated checks using heuristics and prompt engineering, we conducted a manual evaluation of the collected data. For *Initial Contact* and *Financial Loss Metrics*, we calculated data values by manually curating each context. For prompt-engineered queries, we manually evaluated 30%-50% of the data within each narrative sub-category to ensure quality and relevance. Our analysis demonstrated that LLM-based sub-categorical filtering performed effectively across the three categories, and consistently categorizing relevant contexts with high accuracy.

5.2. Results

We present data evaluation and metrics for each category within the narrative analysis of the life cycle of pig-butchering scams. This includes illustrating how scams begin, how scammers build relationships, the aftermath for victims, and the overall tactics used by scammers. The details are provided as follows.

Initial Contact. The victim's shared experience mentioned that scammers often initiate contact with the victim through various dating apps, social media platforms, and accidental text messages. We identified 1,593/2,570 victim sharing being reached out to scammers in 16 distinct platforms. These includes: *WhatsApp* (508), *Instagram* (201), *Telegram* (198), *Facebook* (197), *Tinder* (95), *Match* (48), *Hinge* (43), *Signal* (40), *Linked* (36), and *Twitter* (30), *YouTube* (22), *TikTok* (17), *SnapChat* (10), *Discord* (10), *Google Chat* (10), *Plenty of Fish* (18). We identified 110 victims who mentioned getting text without specifying applications or platforms. We suspect the 110 belonging to phone text messages.

Relationship-Building. We identified 1,427/2,570 victims expressing how scammers build relationships with victims. Based on the analysis, we observe scammers use 10 distinct techniques to build relationships with victims. Among these, the top five techniques are as follows: (i) *Friendship*: scammers often begin as *friends* engaging in casual conversations to build connection (291); (ii) *Romance*: scammers create a romantic atmosphere by discussing dreams of a future together and using affectionate language; (iii) *Trust*: scammers build trust by sharing personal stories, showing empathy, and maintaining consistent communication (278); (iv) *Commitment*: scammers talk about the potential for a committed relationship and promise loyalty (132); and (v) *Future/Connection*: scammers suggest a promising future together, often implying financial security through their connection (74). Examples of victims narratives include:

The scammer shared stories about their family and struggles, making me feel they understood me.

After talking about the future, the scammer told me that for a better retirement I should invest in Hodlsofltd.com.

Scammer Techniques. Of 2,570 victims, 1,175 shared scammers' method of operations that often resulted in financial losses. These include (i) *Fake Investment Platforms*: scammer often directing victims to fake websites/apps (320); (ii) *Advance Fee for Withdrawal*: victims are told they must pay fees or taxes to withdraw funds, with new fees added to withdraw each time (275); (iii) *Cryptocurrency Transfer Requests*: scammers instruct victim to buy cryptocurrency and transfer it to specific wallets under the guise to investment (240); (iv) *Fake Customer Support*: scammers impersonate customer support agents who inform victims of account issues, and agent to resolve the issues (190); and (iv) *Romantic Coercion*: scammers use romantic influence, and convincing victims to investment in securing future together (150). Examples of victims narratives include:

> *When I contacted customer support about withdrawals, they told me my account was flagged and needed a deposit to verify my identity*

> *He told me that if I invested in crypto with him, we could buy a house together and start a life.*

Emotional and Psychological Manipulation. 1,280 victims shared 5 distinct emotional and psychological manipulation techniques that scammers performed. These include (i) *Love Bombing* - scammer expresses overwhelming romantic feeling with victims (340); (ii) *Guilt-Tripping*: scammers make the victim feel guilty in not trusting the scammer (290); (iii) *Urgency and Pressure*: scammers create false sense of urgency and pressured to make decisions in investments or payments (260); (iv) *Isolation*: scammers discourage victim from discussing the relationship or rewards with others (210); and (v) *Future Promises*: scammers promise a future together, and using dreams of shared goals to deepen the emotional attachment and manipulate victims (180). Examples of victims' narratives include:

> *He said our connection was special and private, convincing me to keep it a secret from my friends and family.*

> *We would talk about our future plans, mentioning how investing together would help us buy a house.*

Financial and Psychological Impact. We observe 1,490/2,570 victims shared their life impact related to financial and psychological after being the victim of a scam. In Table 6, we present a breakdown of financial losses by reported currency type. Among these, the victims reported losses in USD was the highest, totaling approximately $1.2 million. Overall, losses were reported in five fiat currencies and three cryptocurrencies, with the total loss estimated at over $5.6 million USD.

We conducted an analysis of the financial and psychological impacts experienced by victims following the scam. These include 5 distinct impact types: (i) *Life Quality and Financial Loss*: victims lose money often from their life savings, and retired plans resulting in life quality ruin (500); (ii) *Debt and Bankruptcy*: victims take out loans or go into debt after the scam, and sometimes result into bankruptcy (320); (iii) *Emotional Trauma*: victims experience severe emotional distress, and feeling of betrayal (270); (iv) *Mental Health Issues*: victims report mental health struggle expressing anxiety, fear, depression and suicidal thoughts (220); and (iv) *Social Isolation*: victims feel ashamed and often felt to remain isolated in social connection due to the fear of guilt or judgment (180). Examples of victims narratives include:

Table 6: Approximated Dollar amount losses from the disclosed victim from public abuse database reports dataset - This table provides reported losses by victims and includes approximated financial losses, with international currencies and cryptocurrencies. In the last row, *Total* we provide the approximated USD dollar values conversion from the first week of November 2024.

Currency	**Approx. Loss Value**	**Victims**
USD	1,200,000	300
EUR	850,000	220
GBP	600,000	180
CAD	500,000	150
AUD	400,000	130
USDT	200,000	90
ETH	300	70
BTC	10	50
XRP	500,000	40
Total (Approx. in $)	5,631,178	1230

> *I borrowed from friends and took out multiple loans. Now, I can't repay them, and I'm facing bankruptcy.*

> *I haven't told anyone about this because I'm embarrassed and afraid of being judged.*

6. Analysis of News Outlets

In this section, we provide the qualitative analysis of 501 news media coverage articles, identifying 50 case studies of 840 victims of pig-butchering to understand the impact of scams especially to uncover patterns in how often victims are reported, the scale of their financial losses, and the detailed tactics used by scammers. We provide further details of our evaluation as below.

Study Setup. We conducted two independent studies on 501 news articles. In the first study, 13 junior researchers from our institution were tasked with labeling each article to determine whether it was related to pig-butchering scams. For articles identified as relevant, the researchers further categorized the information into four areas: (i) *News Details*, which included the publication date and type (general, awareness-focused, or victim-related); (ii) *Victim Details*, which captured information such as the victim's name, age, relationship status, financial loss, career or employment status, and the impact experienced; (iii) *Scam Origin and Scammer Details*, covering the platform used, the country of origin, and the fraud type; and (iv) *Authority Involvement*, noting any law enforcement actions, apprehension of fraudsters, or relief provided to victims. After this initial labeling, a second evaluation was conducted by a senior researcher to assess and address any discrepancies in the data. This thorough review required approximately 41.5

hours of analysis in total, averaging about 5 minutes per article for reading and data entry.

Related News and Filtration. In our news analysis, we identified 397 relevant news articles specifically discussing pig-butchering scams. From an initial selection of 501 candidate URLs, 104 articles were excluded after a qualitative review. These included unrelated news (85), paywall-restricted content (5), unavailable content (7), and geographically restricted content (7), which could not be accessed in our study region. Among the 397 relevant articles, 289 were general or awareness-focused, lacking specific details about victim losses or scam operations. Since our study aimed to examine victim losses and the specifics of scam operations, we focused on 108 articles that included identifiable or anonymized victim narratives. Additionally, we performed two filtration techniques on 108 articles to remove duplicate news based on (i) the victim's name, and (ii) the amount of loss reported. Through such filtration, we obtained confirmed 50/108 case studies of news articles on pig-butchering scams. In the following sections, we provide insights based on these 50 news articles' case studies that were extracted from 501 URLs.

Victim Disclosure and Amount Losses. Among the 50 case studies analyzed, 34/50 disclosed victims identities, while 16/50 were reported anonymously. Within the anonymous category, there were two types of cases: (i) 8/16 involved large groups of pig-butchering scam victims, comprising syndicates with 15 to 482 members, totaling 790 anonymous individuals; and (ii) 8/16 represented individual victims or couples who opted to remain anonymous. Of these 50 case studies, 44/50 case studies specified loss amounts, 5/50 did not disclose the loss amount, and 1/50 case study included narrowly avoided being scammed. Using November 2024 exchange rates, the total reported losses across all cases studied amount to approximately $448,500,944 USD, with an average loss of $9,750,021, a minimum of $7,000, and a maximum of $112,000,000. These figures account for a total of 834 individuals, both with disclosed and anonymous identities while on average the single victim lost $537,770 in pig-butchering.

Victim Demographics. Our study on victim demographics includes details on country, sex, occupation, and age group targeted by scammers: (i) *Country*: We identified 33/50 case studies involving victims from the USA, 12/50 provided by anonymous group case studies from various regions (China, Taiwan, Singapore, Australia, and Malaysia), and 3 from India. (ii) *Sex* Among the cases, 11/50 case studies related to male victims, and 6/50 related to female victims specifically. We suspect the anonymous case studies to contain a mix of both male, female or other identified genders. (iii) *Occupation*: We found that 18/50 cases disclosed the victim's occupation, including retired individuals (2), tech/engineering professionals (4), business/real estate professionals (4), and various other fields such as photography, CEO roles, and culinary, which collectively accounted for 8/18 cases. (iv) *Age*: Sixteen cases specified the victim's age range, between 25 to 89 years, with a median age of 51. This shows that pig-butchering scammers strategically target a diverse range of victims across countries, occupations, and age groups, exploiting personal relationships and trust to manipulate victims into significant financial losses.

Psychological and Well-being Impact. We observed that 14/50 case studies mentioned the impact on victims after the scam. Among these, 1 victim tragically committed suicide after losing their life savings and being unable to support their family, 2 cases reported victims filing for bankruptcy, 3 involved victims losing their homes due to bank debts, and 6 victims lost all their life savings, experiencing severe psychological trauma as a result.

Engagement Platform. In 34/50 case studies provided on how scammers initially contacted victims: (i) 17 of these involved social media platforms such as Telegram, Instagram, WhatsApp, and LinkedIn, (ii) 5 were initiated through dating apps (Tinder, Plenty of Fish), (iii) 6 involved social engineering tactics that directed victims to fake crypto trading websites, and (iv) 3 cases reported initial contact through phone or text messaging.

Scam Techniques and Fraud Schemes. We observe 46/50 case studies provided scammers techniques used as part of their fraud schemes. Among these: 20 involved investment or cryptocurrency fraud, 14 were romance-investment scams, and 12 included various other fraud types, such as job fraud, fake mining schemes, wire fraud/SIM-swap, and property scams. This demonstrates that pig-butchering scams extend beyond romance and investment fraud, encompassing a broader range of social engineering tactics.

Authority and Law Enforcement Enagement. We also investigated the role of law enforcement in apprehending these scammers. In 10/50 case studies, details emerged about law enforcement or court involvement, leading to the arrest of 60 scammers connected to cryptocurrency and investment scams, with a total fraud amount of $172,300,000. These scammers faced charges of conspiracy to commit money laundering, concealing weapons, and fraudulent investment schemes, and authorities uncovered a human trafficking operation from Cambodia, where over 2,000 victims from 11 different countries were being held. Thus, pig-butchering scams are largely sophisticated, syndicate-driven operations, often involving various fraud schemes, money laundering, and even human trafficking networks that exploit victims on an international scale.

7. Scam Tracking and Financial Loss Metrics

We conducted an automated check to identify fraudsters' associated (i) emails, (ii) URLs, and (iii) crypto addresses within our abuse dataset. This section provides an analysis of these fraudsters' communication channels (emails), external connecting platforms (URLs), and payment methods (cryptocurrency addresses) used in their scam operations.

7.1. Fraudulent URLs

From our abuse dataset, we extracted 238 URLs and evaluated them. We provide further details below.

Malicious Check. Acknowledging that not all were linked to abuse sites, we performed a *VirusTotal* scan to check for signs of maliciousness. This scan identified 66/238 URLs as malicious. To further assess their activity, we used Python's *Requests* library to determine if these URLs were live, revealing that 7/66 were still active. We manually visited these 7 sites, identifying 3 as fraudulent investment websites, 2 as fraudulent crypto-draining sites that prompted users to connect their private keys to fake wallet connectors, 1 domain displaying a *403 Forbidden* message, and 1 as fake tech support site with system infected with virus pop-up notifications and link for a download to scan the system.

Registered TLDs. Across these malicious domains, we observed 10 unique top-level domains (TLDs), with the most common being *.com* (48/66), followed by *.cc* (6/66) and *.vip* (2/66).

7.2. Fraudulent Email

From our abuse dataset, we extracted 32 fraudulent emails associated with scammers.

Registration. Of these, 12 were registered to specific domains, while 20 were created through email providers. These providers included *Gmail* (13), *Yahoo* (2), *Hotmail* (2), *Proton* (1), *AOL* (1), and *iCloud* (1).

Keywords. We analyzed the keywords used in these fraudulent email addresses and identified three patterns: (i) 16/32 contained technical support or crypto-related terms like *support*, *info*, *complaint*, *crypto*, and *service*; (ii) 12 used a username format combining a first and last name; and (iii) 3 included terms associated with government programs, such as *enforcement* and *authority*.

Domain Associated and Active Check. Additionally, we checked 12 unique registered domains associated with these emails, among which four were found to be still active. Upon visiting these domains, we found that one displayed blocked content due to an ad blocker, one redirected to a benign page, one was a classic fake tech support site prompting users to call a listed number, and one was linked to a fraudulent crypto exchange.

7.3. Fraudulent Cryptoaddresses

We identified 1,673 crypto addresses in the abuse dataset, of which 1,583 had at least one active transaction recorded on the blockchain. Among these addresses, 3 were Litecoin (LTC) addresses, 749 were Bitcoin (BTC), and the remaining 831 were Ethereum (ETH). We provide our analysis based on transactions from the first week of November 2024, transaction amounts converted to dollar value at the time of each transaction.

Incoming Transactions. These transactions represent the funds received by each account. Collectively, the 1,583 addresses received a total of $629,339,314, with an average incoming transaction amount of $397,561. The highest single incoming transaction was $214,834,563, while the lowest was $1. Notably, 966 addresses received sums below $100 in total, whereas two addresses accounted for 68% ($429,053,245/$629,339,314) of the total incoming funds.

Outgoing Transactions. These transactions reflect the amounts sent from each account. The 1,583 addresses sent a combined total of $380,843,018, averaging $240,583 per address. A single account contributed 53% ($203,103,843/$380,843,018) of all outgoing transactions. Additionally, 93% (1,482/1,583) of addresses recorded outgoing transactions totaling less than $1,000, with an average outgoing amount of $90.

Creation and Last Active Dates. These addresses were created between 2017 and 2024, with the last activity recorded from 2019 through 2024. Among them, 77% (1,231/1,583) were created within the past three years, and 39% (620/1,583) were last active in 2024. We found 193 addresses that transferred out their entire balance after their first transaction, totaling $6,808,300, with an average outgoing balance of $35,276.

Disclaimer. Our evaluation of cryptocurrency addresses is based on publicly reported abuse databases from victim reports, and we acknowledge that not all transactions associated with these addresses may be related to scams. However, we consider these addresses to be highly suspicious and likely misused in fraudulent activities targeting victims.

8. Quantitative Study on Scams

We performed a quantitative study of scams where we surveyed a participants from crowdsourcing platform to identify individuals potentially impacted by scams, including *pig-butchering* scams. Our primary goals were to (i) measure the representative online scam victims of pig-butchering scams in comparison to other types of scams and (ii) perform an in-the-wild quantitative assessment of the financial impacts and losses these scams have caused over the past five years. We provide additional detail on survey setup and findings of participants' responses through the hosted survey as below.

8.1. Survey Setup and Details

Prior to setting up the survey, we conducted preliminary work to refine various aspects, including survey type, model selection, participant demographics, and ethical considerations. We outline the details of these preparations below.

Representational Study and Target Region. We conducted a representative quantitative study, selecting participants from the United States taking into consideration that pig-butchering scams are higher in the U.S. compared to other regions. Acknowledging the limitations in participant diversity on the crowdsourcing platforms, a prevalence study might not accurately reflect users from multiple countries, so we designed our qualitative study to prioritize representativeness over prevalence.

Questionnaires Model. The survey was structured around the following categories: (i) demographics, covering age group, gender, country of residence, and education level; (ii) financial loss, noting any monetary losses due to scams; (iii) scam type, with further questions on contact methods and social engineering tactics specific to targeted scams; (iv) awareness of scams and knowledge of precautions regarding sensitive information sharing; and (v) additional comments or insights on scams. The complete quantitative questionnaire can be found in Appendix C.

Survey Hosting and Response Filtration. We created our survey using *Qualtrics* [86] and distributed it via the crowdsourcing platform *Prolific* [87] in November 2024. A total of 590 responses were received, and we filtered out 6 responses to confirm all participants were from the United States. Our analysis is based on the remaining 584 responses from U.S.-based participants.

Participant Demographics. We ensured all of the participants recruited were from the United States to provide a representative quantitative study. The demographics of participants are as follows: (i) *Age Group*: Participants were distributed across three age groups — *18-24* (278 participants), *25-34* (228 participants), and *35-44* (78 participants); (ii) *Gender*: Participants identified as *Male* (282), *Female* (289), *Prefer not to say* (10), and *Other* (3). (iii) *Education*: The participants' education levels included *High School* (226), *Bachelor's* (263), *Master's* (78), and *Doctorate* (5).

Ethicial Consideration and Data Handling. We consulted our institution's Empirical Research Group to ensure our survey adhered to ethical guidelines, treated participants with respect, avoided sensitive questions, protected data, and upheld integrity. We did not collect any identifying information, such as names, personal references, or other identifiable data. Throughout the survey, we refrained from sensitive questions, including those potentially causing emotional distress or related to cultural contexts, and all questions were phrased in neutral language. Before beginning the survey, participants received a clear description of the study, procedures, and their expected involvement. They were informed they could withdraw at any time, and contact information for the principal investigator and institutional details was provided for any follow-up inquiries. Each survey participant received a $1 compensation, and our participants average time spent was 288 seconds (4.8 minutes).

8.2. Survey Findings

We analyzed the responses from 584 participants, presenting our findings in this section. Our results focus on eight key insights, detailed below.

Online Scams and Defrauded Victims. In our survey, 46% (252/584) of respondents reported being victims of online scams or fraud, while 50% (272/584) indicated they had not been scammed or defrauded in the past five years. Additionally, 10% (60/584) stated they were unsure if they had been scammed or defrauded.

Scam Categories and Frequency. Of the 272 participants who reported being defrauded, 70% (191/272) indicated they had fallen victim to a single type of scam across eight categories: (i) *Phishing* (52), (ii) *Fake Online Website* (44), (iii) *Identity Theft* (30), (iv) *Employment or Job Fraud* (17), (v) *Pig-butchering* (7), (vi) *Charity Scam* (4), (vii) *Technical Support Scam* (3), and (viii) *Lottery/Prize Scam* (2). On the other hand, 44% (120/272) reported being victims of multiple scam types within the past five years. Among these cases, the top three recurring scams were *Phishing* (86/120), *Fake Online Shopping* (54/120), and *Technical Support Scams* (32/120). For participants who experienced repeated scams over the last five years, the reported frequency counts included: two times (67/120), three times (36/120), four times (12/120), and five times (5/120). Additionally, 36 participants described other types of scams, such as credit card theft at gas stations or restaurants, undelivered packages, and phone scams involving fake kidnapping threats.

Amount Lost. In our questionnaires on financial losses from scams over the past five years, users provided responses across various categories: 128 reported no financial loss, 71 lost less than $100, 77 lost between $101 and $1,000, 29 lost between $1,001 and $10,000, and 7 reported losses between $10,001 and $100,000. Based on these ranges, the total estimated losses fall between approximately $106,806 and $1,074,100, with an average loss of $3,209.

Victims of Pig-Butchering Scams. The participant's responses on whether being a victim of pig-butchering scams within 5 years, indicated that 20 participants had fallen victim to pig-butchering scams. Our specific questions on this type of scam uncovered several details: (i) *Method of Initial Contact*: Victims reported initial contact through various platforms, including dating apps (9), social media (6), and other methods (5), such as emails or cryptocurrency exchange websites. (ii) *Victim Grooming Period*: The time scammers spent building trust varied, with 7 participants reporting a grooming period of 1-2 weeks, 5 reporting 3-4 weeks, 2 indicating 1-3 months, and 5 experiencing over 3 months of interaction. (iii) *Reasons for Financial Loss*: Among the participants, 10 reported losses due to fraudulent cryptocurrency investment websites, 6 due to romance scams, and 4 from other types of fraud, including employment scams, cash giveaways, and bank transfers.

Participants' Awareness of Pig-Butchering Scams. A majority of 78% (460/584) of participants reported that they had never heard of pig-butchering scams, while only 14% (85/584) were familiar with this type of scam, and 6% (38/584) were uncertain. These findings highlight a clear need for increased public awareness and education on pig-butchering scams.

Participants' Awareness of General Scams. Among 584 participants, 312 indicated familiarity with online scams. Of these, 34% (106/312) reported being moderately familiar, while 35% (111/312) described themselves as very or extremely familiar. Additionally, 6% (21/312) were not familiar at all, and 23% (74/312) indicated slight familiarity with online scams.

Online Precautionary Measures. We asked participants what precautionary steps they take to avoid being scammed, with five main choices as well as an option for open-ended responses. The responses included: regularly monitoring financial accounts for fraud (75), avoiding sharing personal information (79), educating themselves about new scams regularly (61), verifying unknown contacts across multiple platforms (48), avoiding unsolicited investment opportunities (34), following all the listed measures (12), avoiding downloads (1), and not answering calls from strangers (1).

Additional Comments on Online Scams. We asked participants to provide additional comments or thoughts on online scams and received several such comments. We highlight five main such comments: (i) participants recommended increasing public awareness and education on online scams, especially for vulnerable groups like the elderly, (ii) emphasize the importance of verifying information and being cautious with unsolicited messages, (iii) advocate for stronger laws and enforcement to deter scammers, along with proactive security practices like using strong passwords and two-factor authentication, (iv) staying informed on evolving scam tactics, and (v) supporting victims, and encouraging empathy are also suggested as ways to combat the negative impacts of scams on individuals and society. Examples of comments are as below:

The elder people very vulnerable in these situations. Must be educated by peoples. I always warning my parents about these kinds of scams.

Online scams are more common and sophisticated. Stay cautious, verify sources, don't share personal info, and use two-factor authentication to protect yourself.

9. Discussion

In this section, we provide additional detail on the ethical considerations and limitations of our dataset.

9.1. Ethical Considerations and Disclosure

Our research adheres to strict ethical standards and consulted the internal Empirical Research Team to ensure that our survey questionnaires, models, and data handling comply with data management and *GDPR* guidelines. Prior to the survey, participants were informed about the research goals and data handling practices. We avoided collecting any personally identifiable information and ensured that data collection was conducted anonymously. Furthermore, data gathered from social media platforms, abuse databases, and news outlets consists solely of publicly reported information, with no direct interaction with victims or scammers. We disclosed the scammer's cryptocurrency addresses involved in scams to *Chainabuse* for further action.

9.2. Dataset Limitations

Below we provide limitations on our social media, news, and public abuse report dataset.

Social Media Posts. Our social media data collection was restricted to publicly accessible data that did not require special permissions, memberships, or user-specific relationships to view. We avoided any human interactions during data collection and did not join any social media groups or membership-based communities to collect data. All social media data sources were accessed through APIs.

News Dataset. Our dataset collection relied on news and web searches using three search engines: *Yahoo*, *Bing*, and *Google*. We excluded geographically restricted content and did not crawl data with varied location settings. Consequently, we may have missed news targeted at specific regions or content tailored to particular geographic locations. However, our keyword selection focused on English-language news articles with pig-butchering-specific terms, which means that non-English or region-specific news articles may not be represented in our dataset.

Abuse Dataset. Our public report abuse dataset is based on U.S.-based reports, so the data may not fully represent reports from other languages or regions less familiar with *Chainabuse* and the *Crypto Scam Tracker*. However, we argue that since the U.S. has the highest number of pig-butchering scam victims, these reports likely provide a representative sample of such scams. Although we aimed to collect additional publicly available data for this study, this was not possible. Instead, we collaborated with *Chainabuse*, and the *Crypto Scam Tracker* dataset was publicly accessible, which limited our dataset to these sources. Given that both data sources are leaders in fraud tracking, we believe this data is fairly representative of pig-butchering scams.

10. Recommendations

In this section, we provide recommendations for fighting pig-butchering scams based on the insights collected from the findings of our research. We mainly provide to three different entities: (i) social media platforms, (ii) users, and (iii) policymakers. We provide further details below.

Recommendation to Users. We encourage users to be cautious when responding to messages or unsolicited offers. Scammers often initiate contact through direct messages or public post engagements to lure potential victims with targeted schemes such as romance fraud, investment fraud, or similar scams. Sharing private or sensitive information on social media should be done with care, as scammers may exploit this information to build trust and craft convincing stories, ultimately leading users to fall for pig-butchering schemes. Any investment platforms should be thoroughly verified to confirm their legitimacy. Besides, it is important to perform reverse checks on social media users and associated platforms before engaging in any financial transactions.

Recommendation to Social Media Platforms. We recommend social media platforms regularly monitor profile metadata and user engagement solicitations. We urge online platforms, particularly financial services, and social media sites, to take proactive steps in identifying and preventing pig butchering scams and their variances. These actions should include monitoring user profile metadata connected to external fraudulent websites, cryptocurrency addresses with suspicious or flagged transaction histories, suspicious emails, phone numbers, and similar indicators. Such accounts or content should be blocked or flagged with a potential fraud warning to alert users of potential risks. Accounts engaging with unknown or unverified connections should also be closely monitored.

Recommendation to Policy Makers. As Pig-butchering is a well-planned scam that involves abuse of a multi-layered network, mitigation and safeguarding against such scam requires various policymakers such as government, law enforcement, cybercrime threat intelligence, researchers, social media platforms, and security communities to work collaboratively to tip in any form of suspecting entails. Examples of such regulations include regulating cryptocurrency exchanges, monitoring unusual financial transactions, collaboration with social media platforms, international law enforcement collaboration, streamlining the legal processes such as freezing assets, pursuing criminals, and recovering funds in a timely manner, and ensuring that various sectors are made accountable to fight such scam with regulatory cyber security standards. Through such measures, policymakers can work towards better protecting the potential victims and creating a secure and informed financial environment.

11. Conclusion

In this research, we conducted a comprehensive analysis of pig-butchering scams through previously unexplored sources, focusing on social media, abuse report databases, and news outlets. We identified that scammers employ various social engineering techniques to lure victims across different platforms, extending beyond traditional romance and investment fraud. This large-scale study analyzed victim narratives shared across over 430,000 social media accounts, 770,000 posts, 3,200 abuse database entries, and 1,000 news articles. We uncovered a total of 146 social media accounts, 2,570 abuse database narratives, and 50 case studies of 834 victims who collectively lost over $521 million to pig-butchering scams. Additionally, we tracked fraudulent channels and payment methods scammers directed victims to use. Our quantitative survey on online scams revealed that 50% of the participants had been defrauded in some form, with 20 sharing specific experiences of pig-butchering scams. Based on these findings, we offer recommendations for platforms, users, and policymakers to create proactive defenses against such scams.

Acknowledgements. We extend our gratitude to Ian Schade (Chainabuse) for providing valuable data and insights related to pig-butchering scams and the associated cryptocurrency accounts. We also greatly appreciate the efforts of the students who assisted with the manual review of news articles: Ady, Sagar, Khalil, Abdullah, Alex, David, Keno, Addison, Pouya, Raphael, and Jonathan. This work was funded by the German Federal Ministry of Education and Research (BMBF grant 16KIS1900 “UbiTrans”).

References

[1] B. Blog, “Binance reports a 100% rise in pig butchering scams and shares tips to prevent them.” https://www.binance.com/en/blog/security/binance-reports-a-100-rise-in-pig-butchering-scams-and-shares-tips-to-prevent-them-601342202418225172, 2023.

[2] A. Hetler, “Pig butchering scam explained: Everything you need to know.” https://www.techtarget.com/whatis/feature/Pig-butchering-scam-explained-Everything-you-need-to-know, 2023.

[3] N. Blog, “How to stay safe when having conversations online.” https://www.ncoa.org/article/how-to-stay-safe-when-having-conversations-online/, 2023.

[4] A. Katersky, L. Romero, J. Wagnon Courts, and H. Prince, “Inside the ’crypto con’ costing victims billions in losses: Abc news investigates.” https://abc7.com/inside-crypto-con-costing-victims-billions-losses-scam-compounds-spread-globally-abc-news-investigates/15271293/, 2024.

[5] Z. Faux, “Column: Scam victims may feel stupid. and ashamed. and that’s perfectly normal.” https://www.latimes.com/business/story/2021-04-02/column-scam-victim-feelings, 2024.

[6] NTS, “19 million lose money to scams but fewer than a third report.” https://www.nationaltradingstandards.uk/news/19-million-lose-money-to-scams-but-fewer-than-a-third-report/, 2024.

[7] E. Miller, “Why victims of fraud are hesitant to come forward.” https://www.wtkr.com/news/problem-solvers/why-victims-of-fraud-are-hesitant-to-come-forward, 2023.

[8] J. Munshaw, “”pig butchering” is an evolution of a social engineering tactic weve seen for years.” https://blog.talosintelligence.com/threat-source-newsletter-march-21-2024/, 2024.

[9] D. Nelson, “”’pig butchering’ scams remain dangerous threat in crypto markets, chainalysis report says.” https://www.coindesk.com/policy/2024/08/29/pig-butchering-scams-remain-dangerous-threat-in-crypto-markets-chainalysis-report-says/, 2024.

[10] A. Blog, “The hidden dangers of pig butchering scams.” https://www.aurorait.com/2024/06/26/the-hidden-dangers-of-pig-butchering-scams/, 2024.

[11] A. Blog, “Trash talk: Pig butchering and conversational attacks were the fastest growing mobile threats of 2022 threat insight.” https://www.proofpoint.com/us/blog/pig-butchering-conversational-attacks-fastest-growing-mobile-threats-of-2022, 2023.

[12] A. Hayes, “Pig butchering scams: What they are, warning signs, and how to avoid them.” https://www.investopedia.com/pig-butchering-scams-8605501, 2024.

[13] F. Article, “Romance scams.” https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/romance-scams.

[14] F. Article, “What to know about romance scams.” https://consumer.ftc.gov/articles/what-know-about-romance-scams, 2022.

[15] F. Article, “Investment scams.” https://consumer.ftc.gov/articles/investment-scams, 2023.

[16] D. Article, “Investment scams – what consumers need to know.” https://dfpi.ca.gov/investment-scams-what-consumers-need-to-know/, 2024.

[17] S. Foodman, “Pig butchering crypto scams rising.” https://www.jdsupra.com/legalnews/pig-butchering-crypto-scams-rising-2973108/, 2024.

[18] M. Partners, “Pig butchering crypto scam via whatsapp telegram.” https://mnpartners.in/pig-butchering-crypto-scam-via-whatsapp-telegram/, 2024.

[19] M. Partners, “How one man lost $1 million to a crypto ‘super scam’ called pig butchering.” https://www.forbes.com/sites/cyrusfarivar/2022/09/09/pig-butchering-crypto-super-scam/, 2022.

[20] FinIntegrity, “Pig butchering on the rise.” https://finintegrity.org/pig-butchering-on-the-rise-when-romance-goes-wrong/, 2024.

[21] Y. Bajaj, “New yorkers are mixing love with money, dating app ’pig butchering’ on the rise.” https://www.timesnownews.com/world/us/us-news/new-yorkers-are-mixing-love-with-money-dating-app-pig-butchering-on-the-rise-article-110829541, 2024.

[22] N. Times, “Dating app scam ”pig butchering” hits the netherlands; one rotterdammer lost 14,000.” https://nltimes.nl/2023/06/04/dating-app-scam-pig-butchering-hits-netherlands-one-rotterdammer-lost-eu14000, 2024.

[23] S. Narang, “Pig butchering scam: From tinder and tiktok to whatsapp and telegram, how scammers are stealing millions in a long con.” https://www.tenable.com/blog/pig-butchering-scam-tinder-tiktok-whatsapp-telegram-scammers-steal-millions, 2024.

[24] S. Narang, “Pig butchering scam: How bitcoin, ethereum, litecoin and spot gold (xauusd) investments are used in romance scams to steal hundreds of millions.” https://www.tenable.com/blog/pig-butchering-scam-bitcoin-ethereum-litecoin-spot-gold-xauusd-romance-scam, 2024.

[25] M. Burgress, “The pig butchering invasion has begun.” https://www.wired.com/story/pig-butchering-scam-invasion/, 2024.

[26] T. R. Alber, “The rise of pig butchering scams: A detailed examination.” https://www.linkedin.com/pulse/rise-pig-butchering-scams-detailed-examination-thomas-r-alber-c6goc/, 2024.

[27] R. Lakshmanan, “U.s. authorities seize domains used in ’pig butchering’ cryptocurrency scams.” https://thehackernews.com/2022/11/us-authorities-seize-domains-used-in.html, 2022.

[28] M. Shabi, “The pig butchering: The super scam.” https://knowledge.everc.com/thought-leadership/the-pig-butchering-scam, 2024.

[29] N. Varghese, “Unveiling the pig butchering scam: Deceptive tactics exposed.” https://www.cloudsek.com/whitepapers-reports/unveiling-the-pig-butchering-scam-deceptive-tactics-exposed, 2024.

[30] N. Varghese, “Unmasking pig-butchering scams and protecting your financial future.” https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/unmasking-pig-butchering-scams-and-protecting-your-financial-future, 2024.

[31] F. R. System, “Material loss review of heartland tri-state bank.” https://oig.federalreserve.gov/reports/board-material-loss-review-heartland-tri-state-bank-feb2024.pdf, 2024.

[32] D. Lazarus, “Victim-offender overlap: the identity transformations experienced by trafficked chinese workers escaping from pig-butchering scam syndicate,” 2021.

[33] H.-N. Jiang, C. Wang, and Z.-Z. Duan, “The unpreventable emotional telecom fraud —— ”pig-butchering scam”,” *Scholars Bulletin*, 2023.

[34] M.-H. Maras and E. R. Ives, “Deconstructing a form of hybrid investment fraud: Examining ‘pig butchering’in the united states,” *Journal of Economic Criminology*, 2024.

[35] F. Wang and X. Zhou, “Persuasive schemes for financial exploitation in online romance scam: An anatomy on sha zhu pan () in china,” *Victims & Offenders*, 2023.

[36] M. T. Whitty, “Anatomy of the online dating romance scam,” *Security Journal*, 2015.

[37] X. Tan, “The new network fraud of pig butchering from the perspective of criminal law,” *Lecture Notes in Education Psychology and Public Media*, 2023.

[38] A. Bilz, L. A. Shepherd, and G. I. Johnson, “Tainted love: A systematic literature review of online romance scam research,” *Interacting with Computers*, 2023.

[39] R. Anderson, C. Barton, R. Bohme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage, “Financial cybercrime: Risks, responses and regulation,” *Journal of Cybersecurity*, 2019.

[40] M. Anggusti, “Cybercrime change consumers’ purchase intention in indonesia: a moderating role of corporate social responsibility and business law,” *International Journal of Cyber Criminology*, 2022.

[41] M. Chawki, “Cybercrime and the regulation of cryptocurrencies,” in *Future of Information and Communication Conference*, Springer, 2022.

[42] Chainabuse, “Chainabuse crypto abuse database.” https://chainabuse.com.

[43] C. S. Tracker, “Crytpo scam tracker — department of financial protection innovation.” https://dfpi.ca.gov/crypto-scams/.

[44] S. Lab, “PitButchering Code and Data.” https://github.com/CISPA-SysSec/pig_butchering, 2024.

[45] M. Bartoletti, S. Lande, A. Loddo, L. Pompianu, and S. Serusi, “Cryptocurrency scams: Analysis and perspectives,” 2021.

[46] P. Xia, H. Wang, X. Luo, L. Wu, Y. Zhou, G. Bai, G. Xu, G. Huang, and X. Liu, “Don’t fish in troubled waters! characterizing coronavirus-themed cryptocurrency scams,” in *APWG Symposium on Electronic Crime Research (eCrime)*, 2020.

[47] X. Li, A. Yepuri, and N. Nikiforakis, “Double and nothing: Understanding and detecting cryptocurrency giveaway scams,” in *Network and Distributed System Security Symposium (NDSS)*, 2023.

[48] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy, “Tracking ransomware end-to-end,” in *IEEE Symposium on Security and Privacy (IEEE S&P)*, 2018.

[49] G. A. Siu, A. Hutchings, M. Vasek, and T. Moore, ““invest in crypto!”: An analysis of investment scam advertisements found in bitcointalk,” in *2022 APWG Symposium on Electronic Crime Research (eCrime)*, 2022.

[50] B. Gao, H. Wang, P. Xia, S. Wu, Y. Zhou, X. Luo, and G. Tyson, “Tracking counterfeit cryptocurrency end-to-end,” *ACM on Measurement and Analysis of Computing Systems (ACM MACS)*, 2020.

[51] C. Kuo and S.-S. Tsang, “Constructing an investment scam detection model based on emotional fluctuations throughout the investment scam life cycle,” *Deviant Behavior*, 2024.

[52] T. Buchanan and M. T. Whitty, “The online dating romance scam: causes and consequences of victimhood,” *Psychology, Crime & Law*, 2014.

[53] M. T. Whitty and T. Buchanan, “The online romance scam: A serious cybercrime,” *Cyberpsychology, Behavior, and Social Networking*, 2012.

[54] M. T. Whitty, “Do you love me? psychological characteristics of romance scam victims,” *Cyberpsychology, behavior, and social networking*, 2018.

[55] C. Cross, “Romance baiting, cryptorom and ‘pig butchering’: an evolutionary step in romance fraud,” *Current Issues in Criminal Justice*, 2024.

[56] S. L. Burton *et al.*, “Pig butchering in cybersecurity: A modern social engineering threat.,” *SocioEconomic Challenges (SEC)*, 2024.

[57] C. Cross, “Romance baiting, cryptorom and ‘pig butchering’: an evolutionary step in romance fraud,” *Current Issues in Criminal Justice*, 2024.

[58] M.-H. Maras and E. R. Ives, “Deconstructing a form of hybrid investment fraud: Examining ‘pig butchering’ in the united states,” *Journal of Economic Criminology*, 2024.

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

[60] K. K. Chandra, K. Kalla, J. Bhatia, M. Jayaprakash, and S. R. Dey, "Detection and analysis of cryptocurrency scams on twitter," in *International Conference on Algorithmic Aspects in Information and Management (ICAAIM)*, 2024.

[61] R. Roberts, Y. Goldschlag, R. Walter, T. Chung, A. Mislove, and D. Levin, "You are who you appear to be: A longitudinal study of domain impersonation in tls certificates," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019.

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

[63] A. Rawat, S. Kumar, and S. S. Samant, "Hate speech detection in social media: Techniques, recent trends, and future challenges," *Wiley Interdisciplinary Reviews: Computational*, 2024.

[64] M. Tabassum, A. Mackey, A. Schuett, and A. Lerner, "Investigating moderation challenges to combating hate and harassment: The case of mod-admin power dynamics and feature misuse on reddit," in *USENIX Security*, 2024.

[65] A. Arunasalam, H. Farrukh, E. Tekcan, and Z. B. Celik, "Understanding the security and privacy implications of online toxic content on refugees," in *USENIX Security*, 2024.

[66] M. Franco, O. Gaggi, and C. E. Palazzi, "Characterizing non-consensual intimate image abuse on telegram groups and channels," in *International Workshop on Open Challenges in Online Social Networks (OASIS)*, 2024.

[67] S. Alshamrani, "Detecting and measuring the exposure of children and adolescents to inappropriate comments in youtube," in *ACM International Conference on Information & Knowledge Management (ICIKM)*, 2020.

[68] J. Ratkiewicz, M. Conover, M. Meiss, B. Gonçalves, A. Flammini, and F. Menczer, "Detecting and tracking political abuse in social media," in *International AAAI Conference on Weblogs and Social Media (ICWSM)*, 2011.

[69] G. Gomez, K. van Liebergen, D. Sanvito, G. Siracusano, R. Gonzalez, and J. Caballero, "Sorting out the bad seeds: Automatic classification of cryptocurrency abuse reports," *arXiv arXiv:2410.21041*, 2024.

[70] J. Choi, J. Kim, M. Song, H. Kim, N. Park, M. Seo, Y. Jin, and S. Shin, "A large-scale bitcoin abuse measurement and clustering analysis utilizing public reports," *IEICE TRANSACTIONS on Information and Systems*, 2022.

[71] G. Klein, D. Assadi, and M. Zwilling, "Fighting fire with fire: Combating criminal abuse of cryptocurrency with a p2p mindset," *Information Systems Frontiers*, 2024.

[72] P. Xia, Z. Yu, K. Wang, K. Ma, S. Chen, X. Luo, Y. Zhou, L. Wu, and G. Bai, "The devil behind the mirror: Tracking the campaigns of cryptocurrency abuses on the dark web," *arXiv preprint arXiv:2401.04662*, 2024.

[73] L. Topor and P. Shuker, "Cyber influence campaigns in the dark web," *Cyber, Intelligence, and Security*, 2019.

[74] M. H. Jhaveri, O. Cetin, C. Gañán, T. Moore, and M. V. Eeten, "Abuse reporting and the fight against cybercrime," *ACM Computing Surveys (ACM CSUR)*, 2017.

[75] K. Parti and F. Tahir, ""if we don't listen to them, we make them lose more than money:" exploring reasons for underreporting and the needs of older scam victims," *Social Sciences*, 2023.

[76] 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.

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

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

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

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

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

[82] A. Chris, "Top 10 search engines in the world (2024 update)." https://www.reliablesoft.net/top-10-search-engines-in-the-world/, 2024.

[83] F. Leiser, S. Eckhardt, V. Leuthe, M. Knaeble, A. Mädche, G. Schwabe, and A. Sunyaev, "Hill: A hallucination identifier for large language models," Conference on Human Factors in Computing (CHI), 2024.

[84] D. Khurana, A. Koli, K. Khatter, and S. Singh, "Natural language processing: state of the art, current trends and challenges," 2023.

[85] OpenAI, "Models - openai api (gpt-4o)." https://platform.openai.com/docs/models/gpt-4o.

[86] Qualtrics, "Survey hosting platform." https://www.qualtrics.com/.

[87] Prolific, "Crowdsource platform." https://www.qualtrics.com/.

Appendix

1. Search Keywords Formation

In order to identify posts that are relevant to pig butchering, we initially dive deep into a context that is reported as first-hand experience of pig butchering. Based on such observations, we identified for main categories which are explained further below.

- **Dating/Romance.** We noted that pig-butchering scammers frequently target users seeking dating or romantic relationships through social media. The keywords in this category include phrases such as *find a girlfriend*, *guaranteed sex*, *date Asian*, *mystical romance*, etc. In total, we compiled 49 keywords related to these themes.
- **Investment Fraud.** We observed that social media users frequently fall victim to pig-butchering scams related to investments. These scams involve both traditional investments and cryptocurrencies. Keywords in this category include terms such as *high returns*, *quick gains*, *investment mastery*, *crypto invest*, *double cryptocurrency*, *wealth guard*, and *crypto growth fund*. In total, we identified 100 keywords associated with investment-related fraud cases.
- **Fake Jobs.** We observed that some pig-butchering cases involved scammers offering fake job opportunities. Keywords related to these fake jobs include phrases such as *easy remote job*, *quick job abroad*, *dream careers*, *job security guaranteed*, and *fast track job employment*. In total, we identified 36 keywords associated with fake job scams.
- **Case Studies Track.** We observed that cases related to pig-butchering were often shared as alerts using hashtags. These hashtags/keywords typically included phrases such as *romance scam tracker*, *pig-butchering tracker*, *heartbreak scam warning*, and *fraudulent love alert*. In total, we identified 14 keywords related to popular hashtag case studies.

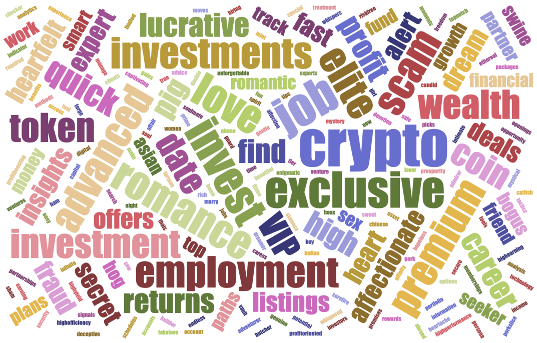


Figure 4: Search keywords word composite: In this figure, we display the word composite used to perform queries for collecting data direct victims of pig-butchering scams. The figure shows that the word composition is higher in contexts related to *investments*, *crypto*, *employment*, *quick wealth*, *romance*, *dating*, *love*, and *career*.

Thus, based on our manual observation, we created a total of 219 keywords that we used as part of search posts on social media platforms. We provide the word frequency composite in Figure 4.

2. Social Media Data Filtration

In this section, we outline the process of crafting prompts to identify posts related to pig-butchering, romance, or investment fraud. We then perform a manual analysis of the responses to verify the effectiveness of this filtration approach. LLMs were selected due to their effectiveness and adaptability in handling a variety of natural language processing tasks, making them particularly suited for accurately classifying fraudulent donation requests. We provide the details of automated and manual filtration below.

Automated Filtration. To determine if a post is related to one of these three cases: pig-butchering, romance scam, or investment fraud, we designed a prompt that evaluates whether the input post includes one of these contexts, outputting the result as a boolean (true or false). Using the OpenAI API [85], we queried each of the posts of four social media platforms. Below, we provide examples of prompt instruction for *pig-butchering scam* along with input samples for responses received in both cases (false and true). We repeat this process for each post to *romance* and *investment fraud.*

Prompt Instruction.

> You are given a text and tasked with determining if it describes a first-hand experience of a pig-butchering scam. The output must be a boolean value, either true or false, formatted as a Python boolean. Provide no explanation.

Input Sample Post - API Response True Case.

> I got scammed by someone claiming to be Drew Barrymore. We had a toured romance through Google chat.. anyway look out much of a bad forgery this is.. @DrewBarrymore

Output of ChatGPT - API Response True Case.

> True

Input Sample Post - API Response False Case.

> Nft and Game are ready to launch as soon as we complete the presale - we will complete the presale in about ... 1 second - so keep your LunarRabbit tokens for gaming experience and great income from activities in the LunarRabbit ecosystem

Output of ChatGPT - API Response False Case.

> False

Manual Filtration. In our manual filtration process, we conduct a qualitative analysis of each post flagged as *true* by the LLM prompt response to further assess whether the narratives align with pig-butchering scams. This filtration process specifically identifies instances where scammers groom the victim before committing fraud, as pig-butchering scams often build upon other types of fraud, such as romance and investment schemes, thus distinguishing them from standard romance and investment scams. Additionally, we performed a random evaluation of the subset cases where LLM responses were *false* and identified that classification held correctness with a negative response.

3. Survey Questionnaires

Our survey questionnaire for participants from *Prolific* was structured around six categories. These categories include: (i) Participant Demographics, (ii) General Questions on Scam Experiences, (iii) Specific Scam Encounters, (iv) Focus on Pig-Butchering Scams, (v) General Awareness & Prevention, and (vi) Closing Questions. The complete list of questions is provided below.

Demographics. In participant's demographics we ask questions related to age group, gender, country of residence, and education level.

What is your age group?

- 18-24
- 25-34
- 35-44
- 45-54
- 55+

What is your gender?

- Male
- Female
- Prefer Not to Say
- Other

What is your country of residence?
(Text Field)

What is your education level?

- No schooling
- High school
- Bachelor's
- Master's
- Doctorate

General Questions About Experiences with Scams. We ask participants whether they have encountered online scams within the past five years.

Have you been scammed or defrauded in the last 5 years? If "No" or "Unsure," you may want to skip them to the end of the survey (#6)

- Yes
- No
- Unsure

How many times have you been scammed or defrauded in the last 5 years?

- 1
- 2
- 3
- 4
- 5
- 5+

How much money did you lose in total due to scams?

- Less than $100
- Between $101 to $1,000
- Between $1,001 to $10,000
- Between $10,001 to $100,000
- Between $100,001 to $1,000,000
- 1 million+
- Did not lose any money

Specific Scam Experience. We ask participants whether they have encountered one or more types of scams from the provided lists of scams.

Which of the following scams have you experienced in the last 5 years? (Select all that apply)

- Phishing (email/SMS)
- Fake Online Website/Shopping Scams
- Lottery or prize scams
- Identity theft
- Charity fraud
- Employment or job offer
- Other (Please specify) [text box]

Focus on the Pig-Butchering Scam. Among the participants who have experienced pig-butchering scams, we ask participants specifics to such scams.

If you selected a Pig-butchering scam, please provide a specific experience. How did the scammer initially contact you? (Social media, Dating app, Messaging app, Email, other)

- Social media
- FDating app
- Messaging app
- Email
- Other (Please specify) [text box]

How long did the scammer build trust with you before asking for money or investments?

- 1-2 weeks
- 3-4 weeks
- 1-3 months
- 3 months+
- Other (Please specify) [text box]

What type of investment did they ask you to make?

- Cryptocurrency
- Stock/Trading
- Real estate
- Other (Please specify) [text box]

Did you report the scam to any authorities?

- Yes
- No

If yes, which authorities did you report it to?

- Local police
- Federal Authorities
- Bank
- Other (Please specify) [text box]

General Awareness & Prevention. We aks participants on whether they were familiar with online scams, and what kind of precautions do they take as part of preventing such scams.

Before you were scammed, how familiar were you with common online scams (e.g., phishing, investment scams)?

- Not Familiar
- Familiar
- Highly Familiar

What precautions do you take now to avoid being scammed? (Select all that apply)

- I do not share personal or financial information online
- I verify unknown contacts through multiple platforms
- I avoid unsolicited investment opportunities
- I regularly monitor my financial accounts for fraud I educate myself about new scams regularly

Closing Questions. Finally, we ask participants if they have heard of pig-butchering scams and invite them to share any additional comments or thoughts on online scams.

Have you heard of the pig-butchering scam before this survey?

- Yes
- No

Do you have any other comments or thoughts on online scams?

[text box]