Navigating the Shadows of Cyber Vigilantism: A Preliminary Analysis of Social Dynamics and Activities of Scambaiting

Manon Berney
manon.berney@unine.ch
University of Neuchâtel
Neuchâtel, Switzerland

Jan Ondrus
ondrus@essec.edu
ESSEC Business School
Singapore, Singapore

Adrian Holzer
adrian.holzer@unine.ch
University of Neuchâtel
Neuchâtel, Switzerland

ABSTRACT

From 2017 to 2022, the Internet Crime Complaint Center documented an increase of 266% complains for online scams. The complexity and constant evolution of these scams pose a challenge for the existing legal system, which appears ill-equipped to effectively combat them. A new movement emerged known as "scambaiting", individuals who autonomously take on the responsibility of advocating for others and fighting against scammers. Leveraging online platforms, these individuals champion causes and educate the public, preventing further victimization. Scambaiting techniques range from entertaining activities, like wasting scammers' time, to illegal ones, such as hacking. This form of cyber-vigilantism represents a novel and under-explored research, especially in term of human-infrastructure. Through the analysis of ten transcripts of discussions involving a sample of scambaiters, we aim to explore the social dynamics and activities of scambaiting; giving insights on collaboration, actors, and challenges within the scambaiting community. Additionally, we present suggestions for future research.

CCS CONCEPTS

• **Human-centered computing** → **Scambaiting**.

KEYWORDS

scambaiting, scamming, online activism, cyber vigilantism, vigilantism, digilantism, virtual communities, social dynamics

ACM Reference Format:
Manon Berney, Jan Ondrus, and Adrian Holzer. 2024. Navigating the Shadows of Cyber Vigilantism: A Preliminary Analysis of Social Dynamics and Activities of Scambaiting. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3613905.3650913

1 INTRODUCTION & RELATED WORK

In 2022, the Internet Crime Complaint Center (IC3) documented 800,000 cases of online complains— an increase of 266% compared to 2017 [27]. This represented a financial impact on victims reaching a record of $10.3 billion in losses [27]. The United Kingdom and the United States emerged as the primary sources with over 600,000 complaints [27]. Conversely, countries such as Nigeria, India, China, and Brazil stand out as hotspots for scammers [8, 16]. The complexity and difficulty of combating scammers arise from factors such as anonymity, strategic tactics, global reach, and legal complexities [7, 16]. The practice of scambaiting emerged as response to these issues, with individuals taking it upon themselves to expose and counteract the tactics employed by scammers [1, 2, 22].

These scenarios, known as "cyber (digital or internet) vigilantism", occurred in the past, where individuals perceived gaps in the legal system and took matters into their own hands. Various forms of cyber vigilantism have been studied, including online shaming, where targets are publicly humiliated on the internet through social media platforms [29]. A recent example is the @CelebJets case, where a Twitter user started posting information on celebrities' private jet flights to shame them for environmental reasons [4]. In some cases, online shaming escalates into "doxing", where users publish personal details online to inflict social punishment on the target [9]. This form of cyber vigilantism can lead to unintended consequences, as illustrated with the example of the Zoe Quinn case, a video game developer, that became the target of online harassment in 2014. The harassment stemmed from false accusations and a controversial blog post by her ex-boyfriend, leading to the public release of her personal information [9, 21]. Another form of cyber vigilantism is hacktivism, defined as the use of computer-based techniques to promote social change. Examples include organisations like "Anonymous" or "WikiLeaks". "Anonymous" engage in various cyberattacks against governments and organizations to advance causes such as free speech and human rights; while "WikiLeaks" publishes classified information to expose government and corporate misconduct [17, 25].

More broadly, Smallridge, Wagner, and Crowl define cyber vigilantism as the act of identifying wrongdoers for social justice using online sources [26]. It often operates informally, outside legal boundaries, and may pose potential harm to targeted individuals [26]. Trottier offers an additional perspective, viewing cyber vigilantism as a form of mediated and coordinated action, where individuals make a target visible online [28]. The characteristics of cyber vigilantism include individual-driven actions, online justice, digital methods, anonymity, unregulated tactics, and its ephemeral nature [26, 28]. In this case, Scambaiting can be defined as a form of cyber vigilantism that aims to expose the tactics used by scammers, wasting their time and resources to hinder future fraudulent activities [31]. While research on cyber vigilantism and scambaiting has explored various theme, such as the methods and tactics employed [13, 33], ethical considerations [6, 12, 18, 19] and conceptualization [11, 26, 28, 32]; the social dynamics of the discipline remains relatively under-studied. Furthermore, scambaiting sets itself apart

CHI EA '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0331-7/24/05.
https://doi.org/10.1145/3613905.3650913

from other cyber vigilantism activities by evolving into a business, with some scambaiters creating content in the form of videos shared on platforms like YouTube, TikTok, or Instagram [24]. This shift resulted in the professionalization of the discipline for some scambaiters. This contrasts with other forms of cyber vigilantism, where the participants often operates in the shadows [26, 28]. Previous work in HCI indicates that the human-infrastructure of a system can be just as important as the technological one [10, 20, 23, 30]. Our work seeks to understand the social dynamics and activities of the scambaiting community. To this end, we explore the following research questions:

- **RQ1:** What are the social dynamics surrounding the scambaiting community? What are scambaiters' motivation and background?
- **RQ2:** How do scambaiters plan and structure their scambaiting activities? What challenges do they face, and how do they manage them?

2 METHOD

To answer these questions, we adopted a mixed-methods research approach [14]. First, to get an overview of the main actors of the movement, we engaged with diverse scambaiting content, spanning podcasts, discussions, videos, and articles. Then, we used the YouTube open API to gather quantitative data (such as follower count, total videos, cumulative views, and channel creation) on popular channels (i.e. channels with the most number of followers) and channels using the following keywords in their channel name "`scambaiting`", "`scambaiter`", "`scam`", "`scammer`". A total of 137 channels were used for the quantitative data collection. The second phase involved the collection of qualitative data. For this, we focused our research on podcasts and discussion from ten scambaiters available online. The scambaiters were selected to represent a sample of the different types of scambaiters according to their level of professionalism, number of followers and techniques. This sample includes two scambaiters with more than 4 millions followers; three scambaiters with over 1 million followers; two with over 1,000 followers, and three with fewer than 1,000 followers. The podcasts were available on different online platform and conducted by individuals not associated with our research team. We then used a thematic approach inspired by Braun and Clark's thematic analysis procedure to analyze podcasts transcripts [5]. This approach includes the following steps: (1) a first-pass listening to the podcasts was used to familiarize ourselves with the data; (2) a first set of code related to our research questions was generated and applied to transcript of the podcasts. Initial codes covered aspects such as scambaiters' "`methodologies`", "`background`", "`motivations`", "`opinions about other members of the community`", "`way of working`" and "`challenges`"; (3) we identified themes based on the codes and common features in the data; (4) themes were discussed and reviewed among researchers; (5) final themes were defined and named and (6) data analysis was conducted.

Ethical approval has been granted for this research (reference 124-2024) by the Research Ethics Committee of the University of Neuchatel (CER-UNINE).

3 PRELIMINARY FINDINGS

This section outlines our preliminary findings derived from both quantitative and qualitative data. We structured the sections to initially focus on the social dynamics of scambaiting and the community surrounding it (RQ1), followed by an exploration of the scambaiting activities, the techniques employed and challenges faced by scambaiters (RQ2). We extracted relevant quotes from the podcasts' transcript to support our findings, and labelled each quote from s1 to s10 to respect anonymity of the scambaiters. We included data on the number of scambaiters (n = x) talking about the findings, if available. Since not all scambaiters discussed them during the podcasts, these numbers should only be considered as informational. Table 1 summarizes the main information about the ten scambaiters and the link to the podcasts.

Scambaiter	Followers	Style	Commitment	Podcast
s1	>4M	Technical	Full-time	Link
s2	>4M	Technical	Full-time	Link / Link
s3	>1M	Social	Full-time	Link
s4	>1M	Social	Part-time	Link
s5	>1M	Technical	Full-time	Link
s6	>1k	Technical	Part-time	Link
s7	>1k	Social	Unknown	Link
s8	<1k	Technical	Part-time	Link
s9	<1k	Technical	Part-time	Link
s10	<1k	Technical	Part-time	Link

Table 1: Information about scambaiters and links to the podcasts

3.1 The Social Dynamics of Scambaiting (RQ1)

Most scrambaiters (n = 8) describe the movement as a niche activity with only a few people actively participating and sharing their experiences on the internet, but it is growing. For instance, in an discussion with the Morning Scam Show, s1 said: *"I think scambaiting is not even close to how it's going to be [in the future] because it still is a niche market, but it will become bigger and bigger"* (s1). And s6 stating: *"I don't particularly recommend picking this niche if you want to be a YouTuber. [...] I think it's still good more and more people do it"* (s6). To illustrate, the graph 1 below, shows the number of YouTube channels opened each year, starting in 2006 until 2023.

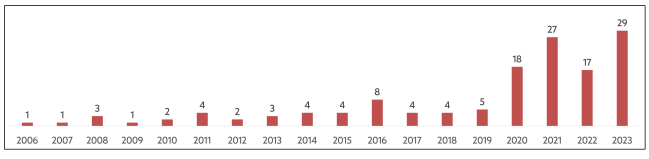

Figure 1: Number of Scambaiting Channels Opened Each Year

3.1.1 ***Motivations.*** Most scambaiters (n = 6) began their scambaiting journeys either because they themselves fell victim to scams or had close associates, like friends or parents, who experienced scams. For instance, s4 initiated her channel shortly after her mother became a scam victim, stating:

> *"my mom fell victim to a scam a few years ago, right before I started my channel and that's what started the first live stream I ever did"* (s4).

Similarly, s5 entered the scambaiting world after nearly falling prey to a scam while trying to sell a camera online. He shared:

> *"I was trying to sell a camera online and someone tried to scam me [...] I didn't fall for it but I realized that a lot of people do fall for these type of things [...] I thought, someone had to get back at these scammers and that's when I made my first video"* (s5).

Other scambaiters (n = 3) embarked on this journey after being influenced by renowned figures in the scambaiting community, such as s8, who was inspired by another scambaiter, Jim Browning:

> *"The things they [scammers] do [in Jim's video] infuriated me. I've always been good with computer and didn't get the change to use that knowledge. So, when I watched that video of Jim, I thought that's an opportunity for me to use that knowledge and help people"* (s8).

And s9, sharing

> *"I was listening to a scambaiter podcast, then saw a Jim Browning video and I was amazed by the level of professionalism there was in his video. He is the one that really got me hooked"* (s9).

Despite varied entry points, a common theme among scambaiters is their shared motivation to help others, highlighted by s3, expressing:

> *"I felt like I wanted to try to call [scammers] and see what I could do to help people"* (s3).

As revealed in an discussion with Fullstack Academy, s2 emphasized that their continued dedication to scambaiting is fueled by:

> *"the thrill of applying my technical expertise to catch a scammer as well as knowing that the work I am doing is making the world a safer place"* (s2).

3.1.2 ***Backgrounds.*** The individuals contributing to the scambaiting movement come from diverse backgrounds. Some possess a technical background (n = 5), others acquire technical skills on the go (n = 2), some (n = 3) do not rely on technical skills for scambaiting. Opinions vary regarding the necessity of a technical background for scambaiting. For instance, s10 believes that having knowledge in IT is crucial before delving into scambaiting, asserting:

> *"I think it [having a technical background] maters actually a lot, because when you're coming in here and messing with people [scammers] you're making them angry and if you didn't protect yourself properly, it can be dangerous"* (s10).

Others leverage their expertise in IT to scambait, as underlined by s1:

> *"[my previous experience in IT security] helped me to learn a lot of tactics on how scammers work and what they do"* (s1).

But don't necessarily think that a technical background in necessary:

> *"There is no need to be technical to be a scambaiter; you just need to keep them long enough on the phone to prevent them from scamming"* (s2).

For instance, s4, formerly a voice actor, leverages their acting skills in videos by creating different personas during scambaiting:

> *"[...] I don't know the first thing about [hacking], I'd rather stick with the comedy aspect"* (s4).

3.1.3 ***A Collaborative Movement.*** Scambaiters (n = 9) also highlight a strong sense of community in the movement. All of them recognize the importance of sharing and collaborating, as underlined by s4:

> *"Out of all content creators, we [scambaiters] don't get upset. The more there are of us, the better it is. No one is upset about copying each other. There is no competition between us"* (s4).

And s1 saying:

> *"We wanna have a spirit of community and everyone rolling together- I like the fact that people that go to my channel also go see other channel, discover other channels through mine"* (s1).

Within this community, scambaiters share techniques, tips, and information about scammers to enhance each other's efforts.

> *"It's nice to have something like a community that share numbers and share information [on scammers], it makes the prep job a lot easier"* (s9).

Moreover, the smaller scambaiters (n = 7) recognize that the the community is centered around the two key figures, Jim Browning and Pierogi. In the discussion, s5 shared their experience during a meeting organized by Pierogi, saying:

> *"I was amazed to see I was worth being involved, it was just cool to see all the preparation that those guy [Pierogi and his team] did [...] and just to have Jim [Browning] there, it was throwing"* (s5).

Furthermore, s6 acknowledged Pierogi as a leader in the movement, stating:

> *"[...] [Pierogi] is definitely a leader, we do look at [Pierogi] as a leader from a small channel perspective"* (s6).

These influential accounts have contributed to elevating scambaiting into a collaborative movement.

3.2 The Activity of Scambaiting (RQ2)

Below, we describe the planning and structuring of scambaiting activity; steps include: (1) preparing the scambait, (2) engaging in scambaiting, (3) sharing. We also discuss investments and risks.

3.2.1 ***Perparing the Scambait.*** In the first phase, scambaiters employ various techniques to locate scammers. One technique includes sharing personal phone number on shady websites, in order for scammers to call it. Consequently, scambaiters like s3, end up on multiple scammer lists, receiving numerous calls daily:

> *"there is a bunch of different ways [to find scammers]. In the beginning it was more hunting them down with weird websites. Now I am on all these scammers lists,*

> *they have list of phone numbers and mine is on all of them. [...]. I can get hundreds of calls per days"* (s3).

Another technique relies on online scammer directories, such as "scammer.info" [1]. Alternatively, some scambaiters wait for scammers to reach them, as discussed by s5:

> *"I don't focus on one area, one country, I just open up my email and try to find something that look fishy and see where it leads me"* (s5).

Scambaiters frequently employ multiple techniques. For more established scambaiters (n = 4), a thorough investigation precedes the interaction with scammers. S2 for instance, admits sometimes spending over six months observing scammers before creating content about them:

> *"Some scammers I've been watching for at least six months before I would put a video out about them. [...] All in all, it can take months and months of work to even get a video live"* (s2).

S1 also invests significant time in gathering personal information on scammers, emphasizing its role in eliciting reactions and instilling a degree of fear by sharing their details:

> *"it [knowing personal information] is part of getting a reaction from the scammers; it's also very important to know what they do, where they live, what they do after and during the scam. I also want to scare them by sharing their information"* (s1).

3.2.2 ***Engaging in Scambaiting.*** In their discussions, scambaiters primarily present two main techniques in scambaiting; hacking scammers (referred to as technical style in table 1) or wasting their time (referred to as social style in table 1). Many find that wasting scammers' time can have a significant impact, preventing them from victimizing others (n = 7). S3 emphasizes this approach:

> *"Most of what I do is try to put them [scammers] into absurd situations and see how far they'll go. I don't hack them, but I stop them from scamming someone else"* (s3).

Others (n = 5) however, employ applications like AnyDesk [2] to access scammers' computers. S8 explains:

> *"All I want from a scammer is an AnyDesk ID"* (s8).

Furthermore, scambaiters adopt varying working styles. While some, like s1, operate as part of a team, the majority work independently (n = 6). Some scambaiters, such as s2, opt for complete anonymity, keeping their channels clear of personal information and avoiding on-camera appearances. Others, like s3, incorporates humor as a key element in its scambaiting approach; for example by using deepfake:

> *"I deepfake my face to look like an old man, so when they [scammers] pull up the webcam, they see an older person and think that I'm an old man with thousand dollars because I also have a fake bank account"* (s3).

3.2.3 ***Sharing.*** In the final step, scambaiters disseminate their efforts by sharing them either with their online community through social media channels and/or with law enforcement. This serves as a crucial step toward progressing to the next stage, aiming to entertain and educate people about scams, and/or facilitate the apprehension of the scammers. S4 underscores the significance of online sharing via social media in the scambaiting process, emphasizing its role in educating people about scams. They devotes considerable time to video editing for this purpose, stating:

> *"I spend a few hours every time to edit the video"* (s4).

And adds:

> *"I take a preventive approach and make people aware and not just laugh"* (s4).

S8 however, prefers to scambait and share information with the police rather than spend time editing videos, noting:

> *"[...] a lot of my time is taken up with editing the videos. Sometimes I don't post on my YouTube channel because it takes too much time editing; I prefer taking that time to scambait"* (s8).

And adds:

> *"Scammers are scared of the police; they do fear people finding out who they are"* (s8).

S1 highlights the importance of collaborating with law enforcement to arrest scammers, explaining:

> *"I go after the bad guys. Scambaiter is not the police, but we can share the information to the fed and then they do whatever they want. Some people were arrested in the US, money-mules for example. Sometimes the shame is worse than jail for the scammers."* (s1).

3.2.4 ***Investments.*** Many scambaiters (n = 5) pursue scambaiting as a side activity while maintaining another profession. For example, s8 shares their experience saying:

> *"For me it's a hobby [scambaiting], I do it Monday to Friday in the UK, start at around 4pm and stop around 10pm. I work during the day and then do it afterwork"* (s8).

Similarly, s10 shares their experience, stating:

> *"I'm just over extended right now because I'm in a busy time in school, I'm taking two classes [...] so I feel a bit overextended so unfortunately scambaiting is losing out right now which sucks"* (s10).

S7 reflects on the effort invested, expressing:

> *"I work harder now than I did when I actually had a good paying job [...] if I were to put this much passion into my job I probably would have been CEO of all the companies I worked for, but it's harder to do that because working at a job isn't as fun"* (s7).

In contrast, larger accounts like s1 or s2 have made scambaiting their full-time commitment, having left their previous jobs. S1 shares their journey, affirming:

> *"I left my job to do this [scambaiting], I'm not going to quit now"* (s1).

[1] https://scammer.info/c/announcements/9
[2] https://anydesk.com/en

In general, the commitment of time, money and resources in scambaiting is substantial within the scambaiters' community. S1 share their experience by saying:

> *"It's expensive to do all these stuff [...] you need to have microphones and fast enough computer [...] and cameras"* (s1).

Furthermore, they dedicated months to learning Hindi specifically for scambaiting purposes, expressing:

> *"I love languages [...] I am really big on culture and wanted to emerge myself into the "why"- why they do scamming, what's the purpose. For this, I had to learn their language"* (s1).

3.2.5 ***Risks.*** Scambaiters unanimously highlight the inherent dangers of this activity, due to potential retaliation from scammers. For example, s1 confesses:

> *"[...] you are dealing with criminals, so we never really advise that people go out and do this themselves"* (s1).

S2 acknowledges the legal concerns with the hacking technique:

> *"[...] when I go back to their [scammers] computer, I don't have their approval and that is illegal. But the only people who could have a problem with that are the scammers. I wouldn't encourage anyone else to do this, and I am taking some risk. But I think the reward [identify the scammers, share information with the police] is worth"* (s2).

S4 expresses caution and opts for a lighter approach without resorting to hacking, explaining:

> *"I don't make anything too serious to make them [scammers] mad. I keep it light. It's not the scammer I'm afraid about but more the people that could stalk me via my channel"* (s4).

To mitigate risks, certain scambaiters establish insider networks in countries such as India or Brazil, where they can safely gather information on scammers and build reliable connections. S6 emphasizes this approach, stating:

> *"I am building an inside network [...] then you have people who you can rely on [...] and they can tell you when there is a really big scam happening"* (s6).

And s10:

> *"I am working with one guy for now, but I hope to someday have a wider network [...] almost like a CIA handler who has a bunch of moles or snitches"* (s10).

4 DISCUSSION

In this paper, we proposed a preliminary study of the scambaiting social dynamics with a focus on the backgrounds, motivation, activity and challenges of scambaiters. We used a mixed-method research approach, with quantitative data collected from the YouTube open API and qualitative data, collected from ten podcasts with scambaiters. Our findings suggest that (1) scambaiting remains a niche activity, attracting individuals from diverse backgrounds, both technical and non-technical, who share the common goal of utilizing their skills to help others; they function as a collaborative community, sharing information on scammers and techniques; (2) the activity of scambaiting can be broken down into three steps: preparing, engaging and sharing; the majority of scambaiters pursue this activity as a side endeavor, facing common challenges related to time, resources, and risks. Those findings are discussed below, with reflection on future work.

4.1 A Growing Collaborative Community

First, scambaiting remains a niche activity, with only a small number of individuals actively participating and sharing their experiences. The community is tightly knit, revolving around two influential figures, who have played pivotal roles in elevating scambaiting into a more professional and collaborative activity. This collaborative spirit is evident in the mutual support expressed by scambaiters, emphasizing a shared goal of helping people and making the online space safer. However, at this stage most scambaiting activities are performed by indiviual scambaiters unlike other more coordinated activist initiatives such as open sources intelligence (OSINT) [3] or digital humanitarian organisations [15].

4.1.1 Future Work. Future research could explore the potential evolution of the scambaiting movement over time and the impact of technological innovation, such as deepfake avatars, voice changer, crowd-sourcing ecosystems, or AI-supported hacking techniques to support their effort at every stage of their activity, from preparing to sharing.

4.2 A Professional Activity

The scambaiting community consists of individuals with both technical and non-technical backgrounds, emphasizing that technical expertise is not necessarily a prerequisite for effective scambaiting. Scambaiters often engage in this activity alongside other professions, and the level of investments vary. However, some of the actors of the scambaiting community manage to turn this activity into a full time job by leveraging the ad-revenues of their social media viewership once they reach a certain level of followers. This opens up avenue for a different form of digital intervention, wherein activists become professionals, thereby potentially extending the duration of the intervention and enhancing its effectiveness.

4.2.1 Future Work. Future research could explore the tension of the business model ecosystem building on a combination of social media influencers strategies paid for by advertisers for an activity which can have ethical and potentially legal implications. Furthermore, future research could explore the impact of long-term digital interventions on behavior change and raising awareness.

4.3 A Dangerous Activity

The scambaiting process involves meticulous preparation, engagement, and post-production efforts, with scambaiters employing various techniques to locate scammers. While some focus on wasting scammers' time to prevent them from victimizing others, others explore hacking techniques, presenting legal and ethical challenges. Indeed, unlike other more professional groups such as OSINTs, scambaiters do not yet have an ethical framework to guide their activities. Furthermore, the dangers associated with scambaiting, including potential retaliation from scammers and risks related

to personal information exposure, influence scambaiters' working styles and levels of anonymity.

4.3.1 Future Work. Future research could further explore pre production processes and the strategies scambaiters employ for self-protection. As mentionned, scambaiters exhibit effective organization and actively exchange information among themselves. Researchers could further explore the information-sharing process, including the tools utilized and methods to enhance effectiveness build ethical guidelines, ensure privacy-by-design and avoid unintended doxing.

5 CONCLUSION & LIMITATIONS

In conclusion, the online scambaiting movement is characterized by a cooperative and supportive community, diverse scambaiting techniques, and scambaiters with distinct motivations and backgrounds. This research provides preliminary insights into a growing and evolving online movement, shedding light on the social dynamics, motivations, techniques, and activities of scambaiters. However, our exploration is limited to a selected group of scambaiters, and the findings may not be fully representative of the entire scambaiting community. Additionally, the discussion on the podcasts were not conducted by the research group, with no control over the question asked and edits, potentially influencing the validity of the information.

REFERENCES

[1] 419 Eater Community. No date. *419 Eater.* https://www.419eater.com/ Accessed: 14.11.2023.

[2] BBC News. 2004. *Nigerian 'email fraudster' arrested.* http://news.bbc.co.uk/2/hi/africa/3887493.stm Accessed: 14.11.2023.

[3] Yasmine Belghith, Sukrit Venkatagiri, and Kurt Luther. 2022. Compete, collaborate, investigate: exploring the social structures of open source intelligence investigations. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–18.

[4] Manon Berney, Jan Ondrus, and Adrian Holzer. 2023. Influencing the Influencers? The Case of @CelebJets and the Role of Social Media in Empowering Citizens to Conduct Climate Justice Activism. In *Proceedings of the Americas Conference on Information Systems (AMCIS)*.

[5] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[6] Stella C Chia. 2019. Crowd-sourcing justice: tracking a decade's news coverage of cyber vigilantism throughout the Greater China region. *Information, Communication & Society* 22, 14 (2019), 2045–2062.

[7] Cassandra Cross. 2018. Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice* 55 (2018), 1–12.

[8] Editorial Desk. 2023. *Top 5 Scamming Countries in the World in 2023.* https://www.techbusinessnews.com.au/top-5-scamming-coutries-in-the-world-in-2023/

[9] David M Douglas. 2016. Doxing: a conceptual analysis. *Ethics and information technology* 18, 3 (2016), 199–210.

[10] Michaelanne Dye, David Nemer, Josiah Mangiameli, Amy S Bruckman, and Neha Kumar. 2018. El Paquete Semanal: The Week's Internet in Havana. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[11] Marta Dynel and Andrew S Ross. 2021. You Don't Fool Me: On Scams, Scambaiting, Deception, and Epistemological Ambiguity at R/scambait on Reddit. *Social Media+ Society* 7, 3 (2021), 20563051211035698.

[12] Matthew Edwards, Claudia Peersman, and Awais Rashid. 2017. Scamming the scammers: towards automatic detection of persuasion in advance fee frauds. In *Proceedings of the 26th International Conference on World Wide Web Companion*. 1291–1299.

[13] Gilles Favarel-Garrigues, Samuel Tanner, and Daniel Trottier. 2020. Introducing digital vigilantism. , 189–195 pages.

[14] Elizabeth J Halcomb and Louise Hickman. 2015. Mixed methods research. (2015).

[15] Adrian Holzer, Bruno Kocher, Samuel Bendahan, Isabelle Vonèche Cardia, Jorge Mazuze, and Denis Gillet. 2020. Gamifying knowledge sharing in humanitarian organisations: a design science journey. *European Journal of Information Systems* 29, 2 (2020), 153–171.

[16] CNA Insider. 22. *India's Thriving Scam Industry: Before You Call Tech Support | Undercover Asia | CNA Documentary.* https://www.youtube.com/watch?v=7CZReZ24-to&t=2018s Accessed on: March 25, 2024.

[17] Adam G Klein. 2015. Vigilante media: Unveiling Anonymous and the hacktivist persona in the global press. *Communication Monographs* 82, 3 (2015), 379–401.

[18] Jeff Kosseff. 2016. The hazards of cyber-vigilantism. *Computer Law & Security Review* 32, 4 (2016), 642–649.

[19] Samuli Laato and Sampsa Rauti. 2021. Scambaiting as a Form of Online Video Entertainment: An Exploratory Study. In *Proceedings of the 12th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2020) 12*. Springer, 738–748.

[20] Charlotte P Lee, Paul Dourish, and Gloria Mark. 2006. The human infrastructure of cyberinfrastructure. In *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work*. 483–492.

[21] Karla Mantilla. 2015. Gendertrolling. (2015).

[22] Youngsam Park, Jackie Jones, Damon McCoy, Elaine Shi, and Markus Jakobsson. 2014. Scambaiter: Understanding targeted nigerian scams on craigslist. *system* 1 (2014), 2.

[23] Javier Pastor-Galindo, Pantaleone Nespoli, Félix Gómez Mármol, and Gregorio Martínez Pérez. 2020. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access* 8 (2020), 10282–10304.

[24] Rest of World. 2023. *The YouTube Vigilantes Chasing Down Scam Callers.* https://restofworld.org/2023/youtube-scam-call-vigilantes/ Accessed: 14.11.2023.

[25] Micah L Sifry. 2011. *WikiLeaks and the Age of Transparency.* OR Books.

[26] Joshua Smallridge, Philip Wagner, and Justin N Crowl. 2016. Understanding cyber-vigilantism: A conceptual framework. *Journal of Theoretical & Philosophical Criminology* 8, 1 (2016).

[27] The Federal Bureau of Investigation. 2022. *Internet Crime Complaint Center (IC3) 2022 Annual Report.* https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[28] Daniel Trottier. 2017. Digital vigilantism as weaponisation of visibility. *Philosophy & Technology* 30 (2017), 55–72.

[29] Daniel Trottier. 2020. Denunciation and doxing: Towards a conceptual model of digital vigilantism. *Global Crime* 21, 3-4 (2020), 196–212.

[30] Sukrit Venkatagiri, Aakash Gautam, and Kurt Luther. 2021. Crowdsolve: Managing tensions in an expert-led crowdsourced investigation. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–30.

[31] VICE. No date. *The YouTuber Exposing Scams as a Scambaiter.* https://www.vice.com/en/article/93w8pe/youtuber-exposing-scams-scambaiter Accessed: 14.11.2023.

[32] Elizabeth Yardley, Adam George Thomas Lynes, David Wilson, and Emma Kelly. 2018. What's the deal with 'websleuthing'? News media representations of amateur detectives in networked spaces. *Crime, Media, Culture* 14, 1 (2018), 81–109.

[33] Andreas Zingerle and Linda Kronman. 2013. Humiliating entertainment or social activism? Analyzing scambaiting strategies against online advance fee fraud. In *2013 International Conference on Cyberworlds*. IEEE, 352–355.