DOI: 10.1111/1745-9133.12684

CRIMINOLOGY & Public Policy

ORIGINAL ARTICLE

Lessons learned from Dread darknet communities: How and why are fraudsters targeting the elderly to be victims or accomplices?

Kenji Logie | **Sumita Das**

Department of Criminal Justice, John Jay College of Criminal Justice, New York, New York, USA

Correspondence
Kenji Logie, Department of Criminal Justice, John Jay College of Criminal Justice, 524 West 59th Steet, New York, NY 10019, USA.
Email: klogie@jjay.cuny.edu

Abstract

Research Summary: We examined darknet user discussions on the Dread forum to identify key themes and emerging topics in fraud planning, focusing additionally on elderly victimization. Using the conceptual framework of criminogenic learning to study the process of fraud planning in darknet communities of practice, we analyzed the content of original user posts (n = 818) and comments (n = 1365) collected from the Dread forum. We identified nine unique fraud categories, of which payments-related fraud was the most-discussed fraud category and accounted for 25% of original user posts. We further found our sampled forum content to be dominated by the theme of learning or knowledge sharing in eight of the nine fraud categories, which appeared in more than 44% of original user posts. Our content analysis revealed specific insights into why and how darknet forum users may target people, including the elderly subpopulation, for different types of fraud. Overall, our research demonstrates the diversity of opinion and knowledge sharing among darknet forum users in relation to planning and committing fraud against the elderly, views on who is a suitable target and why, and what veteran and aspiring fraudsters consider to be important information for success in fraud.

Policy Implications: Utilized independently or as part of a multistage strategy of darknet data analysis, our research method can be used to monitor criminally active darknet forums for current and emerging themes in fraud against general populations and vulnerable subpopulations, such as the elderly, and to develop strategies to identify, disrupt, or destroy hubs of criminal planning and knowledge sharing. Our study additionally informs policy makers of certain elder-specific vulnerabilities that might be addressed by more up-to-date elder cybercrime awareness campaigns and initiatives. Our findings also highlight the presence of insider threats that may inform discussions on how health and financial institutions can better regulate these cybersecurity risks.

KEYWORDS
darknet, elderly, forum, fraud, knowledge sharing

The Internet is an indispensable part of modern life. It is estimated to have grown to 5.3 billion global users in 2023 (Cisco, 2020), with users relying on various Internet-driven or Internet-enabled activities such as digital payments. Digital payments alone are globally projected to grow from $3.5 trillion in 2018 to $19.9 trillion by 2026 at a compound annual growth rate of 24.4% (Fortune Business Insights, 2020). This growth has been accompanied by steep increases in cybercrime losses from cyberattacks and cyber-enabled fraud incidents (Hasham et al., 2019), with a recent World Economic Forum report (2023) ranking "widespread cybercrime and cyber insecurity" (p. 6) as one of the top 10 global risk categories in both the short and long terms. Fraud has emerged as one of the most important types of cybercrime globally because of the growth in Internet users (Buxton & Bingham, 2015; Cross, 2022; Mikhaylov & Frank, 2016; Rehman et al., 2023). Between 2019 and 2023, the Federal Bureau of Investigation (FBI) received a total of 3.8 million complaints from business entities and individuals against cyber incidents or cyber-enabled fraud, with losses estimated at $37.4 billion (FBI, 2024).

Cyber-enabled fraud is a relatively new type of crime, with criminals creating and adopting novel methods of victimization faster than policies can be designed and implemented and law enforcement can act. Currently, the FBI's Internet Crime Complaint Center (IC3) tracks approximately 26 categories of cybercrime complaints, including several cyber-enabled fraud categories. Their most recent report of complaints received in 2023 suggest that elderly populations may be especially vulnerable to cybercrime and cyber-enabled fraud. In 2023, an estimated $3.4 billion was lost by 101,068 elderly victims aged 60 and above, accounting for the highest share (24.1%) of complaints by an age group as well as the highest share of financial losses (41.5%) by an age group (Internet Crime Complaint Center, 2024). The report also shows that members of the 30–39 (88,138 complaints and $1.1 billion in losses) and 40–49 (84,052 complaints and $1.5 billion in losses) age groups filed less complaints while losing less money as a group and even per victim

compared to victims in the 60 and above age group. Elderly victimization is therefore of special importance in conversations focused on improving how we respond to the growing and evolving threat of cybercrime and cyber-enabled fraud.

In a growing number of studies, darknet spaces and their role as hubs for planning criminal activities, sharing of criminal enterprise knowledge, and enabling communities of practice (CoPs) have been identified (Chertoff & Simon, 2015; Duxbury & Haynie, 2018; Holm, 2017; Logie et al., 2023; Maras et al., 2024; Mirea et al., 2019). In this paper, we conceptualize the darknet forum as a learning-oriented virtual CoPs (Henri & Pudelko, 2003) that enables members to create and share criminogenic knowledge. This knowledge sharing is dominant during the fraud discovery phase, which determines how a fraud scheme is developed and the level of success achieved utilizing the scheme (Albrecht et al., 2011). Our research incorporates data from the darknet forum Dread, specifically covering the timeframe from 2020 to 2023. We aim to analyze the thematic content of a carefully chosen sample of discussions related to fraud. Through this analysis, we seek to understand how darknet forum users may be utilizing these discussion platforms to learn collaboratively, share knowledge, and even develop novel thought experiments about fraud-related crimes.

1 | CONCEPTUAL FRAMEWORK AND LITERATURE REVIEW

The darknet represents a small but highly active cyberspace underground, invisible to most users except those with access and knowledge of special browsers such as Tor, Freenet, or I2P that allow users to stay undetected and anonymous (Maras, Arsovska et al., 2023; Pete et al., 2020). Therefore, marketplaces, forums, groups, and user activities on the darknet are hidden from law enforcement and formal regulatory authorities. This makes the darknet highly attractive to a variety of users who wish to deliberately obfuscate their presence or engage in illegal activities (Chertoff, 2017; Mirea et al., 2019). Holt et al. (2015) observed that the extremely clandestine and under-radar nature of transactions in darknet marketplaces reduces even the perceived efficacy of law enforcement to "disrupt or otherwise impede the practices of market actors" (p. 96), as a result of which law enforcement may need to resort to unique and disruptive mechanisms to "disrupt the practices" of offenders, such as undercover identities of surveillance and forum creation, and slander attacks on seller reputation. Forums, on the other hand, may serve a variety of purposes including marketplace trading (Bermudez-Villalva & Stringhini, 2021) and as knowledge repositories (Wasko & Faraj, 2000).

Knowledge sharing occurs on both darknet marketplaces and darknet forums and may take on a more formal structure when created within the criminal organization and maintained by it (Logie et al., 2023; Maras et al., 2024). A recent study (Kwon et al., 2020) highlighted the importance of knowledge creation and sharing among criminal groups; when criminals obtain access to virtual forum, they may utilize the platform to collaborate with potential co-offenders, learn from mentors, or obtain materials for self-directed learning from the community (Goldsmith & Brewer, 2015; Holt et al., 2010; Hutchings & Holt, 2015; Leukfeldt et al., 2017; Soudijn & Zegers, 2012; Weulen Kranenbarg, 2022; Weulen Kranenbarg et al., 2021). Leukfeldt et al. (2017) even described the darknet discussion forum as a "university for cybercriminals" (p. 17) that helps curious members and aspiring criminals learn the tools of the trade, obtain domain knowledge to understand security vulnerabilities better, and access other educational materials to self-learn.

Forums as knowledge repositories, whether hosted on the surface web or the darknet, may facilitate the creation, transmission, sharing, and exchange of knowledge, skills, and ideas among

users. Specific to darknet forums, studies have described their role in transmitting knowledge, from more experienced criminals to newcomers or those with less experience, indicating that the darknet forum may potentially help criminals to develop and plan their crimes (Jordan & Taylor, 2017; Shakarian et al., 2016). Nurse and Bada (2019) also described the environment in darknet forums as one promoting the exchange of information and learning kits, even implying that some darknet forums may be intentionally designed to follow a cybercrime-as-a-service (Manky, 2013) business model. Nurse and Bada (2019) additionally highlight the role of trust in darknet forums as an "enabler of online engagement," which could result in member behaviors such as staying anonymous to avoid detection by undercover law enforcement officers, decisions on outreach to other members, and decisions on which learning resources to access.

1.1 | Insider versus outsider alternative pathways to criminogenic knowledge framework

In a recent study, Allan (2018) examined Australian criminal investigation data from 19 cases involving financial crime or fraud to understand how the principal offenders obtained criminogenic knowledge and access to commit crimes. This study identified the following learning-based sources of criminogenic knowledge: (1) formal education, (2) occupational learning directly as an insider threat employee or through close interaction with other insider threat employees, (3) exposure to offending methodologies or investigative practices, or (4) through typically fee-based services facilitated by an expert.

Allan (2018) developed a framework to account for how criminals acquire the knowledge to commit crimes. Although his research focused on how organized crime groups and their members participate in financial crimes, his recommendations can also be applied to individual learning. Allan proposed that in order to understand fraud and financial crimes, it is necessary to grasp the concepts of access, learning, planning, and implementation, as well as to consider the roles of the crime type itself and the criminal's level of access and understanding of crime-detection systems in each of these stages of committing the fraud and financial crime. Allan (2018) further noted that the level of knowledge available to a perpetrator depends on whether they are an insider or outsider and the specific group they belong to within these two classifications. Insiders primarily consist of three types: (1) Internal Masters who are experienced, possess insider knowledge, and have high-level access within the organization, (2) Internal Learners who are individuals with less experience, less knowledgeable, and lower level access within an organization, and (3) Insiders who are individuals used by Internal Masters and Internal Learners, who are part of another organization, and who possess the knowledge or information required to fill any gap inhibiting the successful completion of a crime by an Internal Master or Internal Learner. Outsiders are also divided into three subgroups: (1) Outsider-Victim is a perpetrator who directly interacts with the victim organization, (2) Outside-Associate-Victim is an outsider who utilizes other associates to interact with the victim organization, and (3) Outsider-Insider-Victim is a perpetrator who uses an insider from another organization to acquire the knowledge required to successfully commit crimes against the victim organization.

Allan (2018) identifies that an offender's access is determined by their position as an insider or an outsider in the organization, but their knowledge is obtained through traditional learning sources or alternative learning sources. Traditional learning sources include formal education and on-the-job training. In contrast, alternative learning sources include exposure to criminal methodologies and investigative practices, criminal facilitators, and darknet CoPs. In the context

of learning facilitated through a darknet forum, criminal facilitators and darknet CoPs are the most important of these learning mechanisms. A criminal facilitator is an individual who provides knowledge and insight for the commission of a crime including how to commit crimes, telecommunication expertise, and insights into an organization system's internal structure and vulnerabilities. Darknet CoPs are described as the community domain and practice, where all current members including criminals are allowed to learn a number of skills and gain knowledge in a social environment. Individuals actively seek out knowledge in this environment and darknet forums in alignment with learning theory (Akers, 1973; Sutherland, 1947) and consistent with the concept of learning as a "fundamentally social phenomenon" in CoPs (Wenger, 1998). Finally, Allan noted that outsider threats tend to seek knowledge primarily from alternative learning sources, whereas insiders primarily use traditional learning sources to commit crimes.

The current study builds on Allan's framing of fraud-related learning sources, specifically the concept of darknet communities being used to facilitate learning and specialized knowledge sharing, while acknowledging that fraudsters may be able to utilize other sources of learning to plan their crime.

1.2 | Darknet forums as virtual CoPs to develop fraud schemes

Wenger (1998) first proposed the concept of CoPs to describe a group whose members are bound informally by shared intention of activities and mutual engagement in these activities that result in the production of some capability such as learning. Three dimensions define the shared practice of CoPs: (a) the goal or purpose of the joint enterprise as understood and renegotiated by the community members; (b) the relationships and bonds of mutual engagement that bring and keep the members together as a group; and (c) the shared communal repository of capabilities and resources developed by the members throughout time. Henri and Pudelko (2003) attempted to apply Wenger's CoPs theory of learning as a social system to the virtual community. Observing that the activity of virtual community participants may be associated with formal or informal learning (Trentin, 2001), socialization (Gordin et al., 1996), or indirect learning (Nichani & Hung, 2002), they developed a typology of virtual communities. Based on the strength of the community's intentionality or goal of existence (weak to strong) and the level of bonding or cohesion of the groups (low to high), the following types of virtual communities were proposed: (1) community of interest (weak shared goals, low cohesion), (2) goal-oriented community of interest (moderate shared goals, moderate cohesion with a short-term mandate), (3) learner's community (moderate shared goals, high cohesion dependent on the ability of the educator), and (4) CoPs (strong shared goals, high cohesion). These have implications on the type of learning expected to emerge from community participation. For example, the learning in a community of interest would consist of "knowledge construction, the use of which is more personal than collective" (Henri & Pudelko, 2003, p. 478). In CoPs, the learning is expected to be collaborative and supported by members' sense of a professional community identity with specific criteria and rules, their identification with a common practice, their recognition of common goals or needs, the acceptance of change through contact with others, and the goal to gain or improve competencies.

Most of the existing literature on darknet forum processes rely on the conceptualization of the darknet forum as virtual CoPs. A recent study by Maras et al. (2024) observed that CoPs are present in darknet forums and occur when darknet users with a shared interest in a topic create informal networks (subforums or threads) to create and share knowledge about a specific issue through

an iterative process. Their research further suggested that the CoPs concept, with its implications of community belongingness and continuous learning of "public goods" knowledge, could make darknet forums resilient against law enforcement tactics of marketplace shutdowns or the arrest of individual members. In the absence of longer term strategies of disruption, darknet CoPs are likely to recover or regroup in existing darknet spaces by multihoming or migrate to new darknet marketplaces (Calis & Tsekouras, 2018; Maras, Logie et al., 2023) and remain one step ahead of law enforcement. To "counter the persistence and expansion of these illicit markets," Maras et al. (2024) recommended that law enforcement monitor criminal groups of interest on the darknet and their CoPs learning and knowledge sharing processes.

1.3 | Study focus: The Dread darknet forum

Forums come in various forms and sizes. Although some focus on a single issue, others have multiple subforums or discussion boards (Holt, 2013; Howell et al., 2023; Kigerl, 2018). This study focuses on the learning and knowledge-sharing mechanisms observed in the Dread forum. Dread is one of the oldest darknet forums launching in February 2018 (see Appendix A). Dread allows users to join public and private (by invite only) specialized knowledge or general subforums. The subforums include darknet marketplaces, hacking, ID theft, fraud, and drug subforums. In addition to the forum service, Dread, through a subsidiary service, also offers one of the largest searchable darknet market vendors database.

The Dread forum was created in response to the crackdown on various Reddit subforums, specifically ones dedicated to darknet marketplaces and criminal knowledge sharing such as "fakeid." Dread has been described as a Reddit hidden service by its founder and early adopters. It was positioned as a new home for many of the displaced darknet Reddit subforum members. Its founder and early adopters also perceived it as necessary to allow free speech without censorship to continue. Since its inception, Dread has relied heavily on donations from its members. Recently, it has also generated income from the sale of premium memberships, awards, and advertisements to offset the cost of forum operations. Finally, like many successful darknet sites, the Dread forum has been subject to Distributed Denial of Service (DDoS) attacks and other sophisticated attacks against its servers and services. In response, forum administrators have had to take the forum offline multiple times to make service and security upgrades.

On Dread, topic-specific forums and subforums serve as CoPs where knowledge sharing occurs in the discussion threads of these specific forums. Based on registered members who have joined the top 10 Dread subforums, the forum discussions appear to be dominated by topics of fraud, darknet marketplaces, and drug quality (see Appendix B). Forum participants[1] include (1) general members who can create and share user-generated content or posts, (2) content administrators who create guides and rules for proper use of the forum, and (3) subforum moderators who are allowed to create more specific guidelines and rules for their specific subforum. More sophisticated moderators may be able to use bots on their subforums to operationalize rules and guidelines and even to optimize knowledge sharing. The Dread forum offers its members the advantages of subject-specific or curated content, multiple knowledge-sharing mechanisms, and quality optimization tools or resources such as bots, guidelines, and rules (see Appendix C). The Dread forum is an example of darknet CoPs that supports learning among its members through the creation and sharing of knowledge.

1.4 | Review of relevant fraud studies

There is an extensive body of research from the last three decades that explores different fraud methods, victims, and offenders in the real as well as virtual world. There is also a growing body of research dedicated to understanding frauds committed against the elderly, given the rise in the number of victims in this subpopulation. Below, we explore current and existing research into traditional fraud and how they are similar or different in the virtual environment.

1.4.1 | Fraud

Fraud is described as a criminal act involving intentional deceit, dishonesty, or trick to gain knowledge or financial advantage (Akers & Gissel, 2006; Akinladejo, 2007; Cole & Miller, 2023; Cross, 2022; Gillespie & Magor, 2020; Kemp et al., 2020; Rose, 2018; Vaisu et al., 2003). Fraud has been grouped into three broad categories that take into consideration the environment and method used to commit fraud—traditional, cyber-enabled, and cyber-dependent (Button & Cross, 2017; Cole & Miller, 2023; Holt et al., 2010; Levi et al., 2017; McGuire & Dowling, 2013). Fraud crimes have also been subdivided based on the characteristics of the fraud into seven categories: consumer investment fraud, consumer products and services fraud, employment fraud, prize and grant fraud, relationship and trust fraud, phantom debt collection fraud, and charity fraud (Beals et al., 2015; Gillespie & Magor, 2020; McGuire & Dowling, 2013). Researchers later identified identity fraud as an eighth category (Button & Cross, 2017; Kemp et al., 2020).

1.4.2 | Identify theft fraud cycle

Albrech et al. (2011) in their study acknowledged that the Internet has increased access to victims' personal information, enabling perpetrators to engage in fraud through a multistage identity theft fraud cycle (e.g., fraud cycle). Although the full cycle consists of the three stages of Discovery, Action, and Trial, a fraud may not involve all stages, depending on the type of fraud and the perpetrator's level of success in each stage. In the initial Discovery stage, the perpetrator acquires and verifies information about a potential victim. In a traditional Discovery stage, perpetrators acquire individual victims' information using techniques like carding, phishing, computer searches, or some other method such as searching a victim's home or trash; once the data are collected, they may be verified by telephone scams. Today, the Internet offers a perpetrator many additional tools to verify the information during Discovery or later stages in the fraud cycle. The second stage, referred to as Action, involves the perpetrator obtaining the necessary tools and resources to effectively carry out the fraud. These are the preparatory steps taken prior to the actual execution of a fraud. The action stage additionally entails the implementation of concealment strategies that obstruct the victim's ability to detect an ongoing fraud, thereby enabling the perpetrator to conduct the fraud during an extended duration. The final stage, known as Trial, is characterized by three sequential phases that progressively escalate the victim's financial loss. The first phase, referred to as first-dimensional action, involves the perpetrator testing stolen information through low-risk transactions that do not require face-to-face interactions. This enables the offender to determine if the information and credit card are usable or should be discarded, and then to begin a new cycle of fraud with a different victim. Any actions carried out subsequent to the designated testing period during the first-dimensional action, leading to benefits for the perpetrator, are considered second-dimensional actions. This may include larger purchases, typically items with a

value below $1000 that do not involve recurring or accruing charges billed to accounts. If the purchases made during the second-dimensional action are successful, the perpetrator may proceed to third-dimensional action and pursue higher financial rewards by making even larger purchases, which require financing or the establishment of credit card and bank accounts. When an offender is successful, they will dispose of the victim's information and proceed to restart the cycle, using the identity of a different victim.

1.4.3 | Routines and behaviors

Darknet spaces offer anonymity, invisibility, asynchronous remote capabilities, and direct person-to-person interactions, translating to reduced risk for the cybercriminal to be detected or retaliated against (Capeller, 2001; Holt et al., 2015; Wang et al., 2020; Yar, 2005). These factors may limit the effectiveness of cybercrime prevention strategies rooted in anti-victimization frameworks—for instance, the framework of routine activities theory (RAT; Cohen & Felson, 1979), which offers three potential pathways to prevent victimization by (1) increasing the effort required to offend, (2) increasing the risk of getting caught, or (3) reducing the rewards of offending (Choo, 2011). Overall, studies offer mixed support for the use of RAT-informed measures to prevent cybercrime victimization (Bossler & Holt, 2009; Choi, 2008; Choo, 2011; Grabosky, 2001; Leukfeldt & Yar, 2016; Marcum et al., 2010; Newman & Clarke, 2013; Ngo & Paternoster, 2011; Yar, 2005). Although RAT-based studies improve our understanding of cybercrime victimization risk profiles and how user vulnerabilities can be addressed through cybersecurity and self-protection (Leukfeldt & Yar, 2016; Marcum et al., 2010; Pratt et al., 2010; van Wilsem, 2011, 2013), they offer limited guidance for cybercrime control efforts that can be utilized by law enforcement practitioners.

To effectively control cybercrime and cyber-enabled crime, law enforcement strategies need to consider the offender's perspective, using a process-based conceptual framework to understand "how" and "why" they plan their schemes of crime instead of focusing primarily on "who" they target and for "what." Process-based and offender-focused frameworks of learning and knowledge sharing may be particularly well-suited for law enforcement to adopt in their efforts to understand criminal planning on darknet spaces.

1.4.4 | Victimization of the elderly subpopulation

Specific to the subpopulation of elderly or "older" persons, typically defined as individuals aged 60 years or more, several studies till date have highlighted important elderly specific risk factors and vulnerabilities for cybercrime including cyber-enabled fraud, such as lower self-control (Holtfreter et al., 2015), age-related cognitive decline and susceptibility (DeLiema, 2018; James et al., 2014), low understanding of risky Internet activities (Cross, 2017; Elueze & Quan-Haase, 2018), overconfidence in digital literacy or financial decision making (Parti, 2023), social isolation or living alone (DeLiema, 2018; Fenge & Lee, 2018), and major disruptions to routines and support structures (Huey & Ferguson, 2022), including retirement (Morrison et al., 2020) and COVID-19 (Auer et al., 2020; Cross, 2021; Morrison et al., 2023). On the other hand, some studies also showed that older individuals consume information from traditional media rather than digital media, with the exception of individuals with higher levels of education (Bachmann et al., 2010; Diehl et al., 2019; Mears et al., 2016), which may translate to a somewhat protective effect for elderly populations.

Finally, underreporting of elderly fraud remains a persistent issue (Beals et al., 2017; Fitzpatrick & Hamill, 2010; Gu, 2021; Mears et al., 2016; Ross et al., 2014). Whether based on poor survey design, forgetfulness, lack of knowledge, or a feeling of shame, older adults underreport fraud on surveys. Fear of discussing financial loss with their family members or of being disowned by the family members could also contribute to the underreporting of fraud by the elderly (Button & Cross, 2017; Fitzpatrick & Hamill, 2010; Gu, 2021).

1.5 | Significance of the current study

Cybercrime is a growing threat that many believe to be driven by rogue and malicious actors operating on the darknet. Our study adopts a broad conceptualization of darknet forums as virtual communities that function as social learning entities and whose members voluntarily create and share criminogenic knowledge to be used in the planning and implementation of financial crime. We primarily explore how fraudsters utilize the darknet forum as a platform to learn, share knowledge, and potentially collaborate on fraud schemes. By exploring how darknet forum members discuss the elderly and use forum threads to talk about fraud, we hope to add not only to the limited existing literature on elderly cyber-enabled fraud victimization but also to the broader literature on how cyber fraudsters may be utilizing darknet forums to develop and conduct fraud schemes.

Elderly individuals are at high risk of cyber or cyber-enabled frauds, either due to targeted fraud schemes or routines and behaviors, and they experience greater financial losses affecting the quality of life for victims in this vulnerable population. Although most studies on elderly cyber victimization have focused on their risks and vulnerabilities due to routines and behaviors, we are not aware of any recent study that examines how offenders develop fraud schemes specifically targeting the elderly.

This study offers a novel perspective on elder-targeted cyber-enabled fraud victimization. Coming at a time when the elderly in the United States are both increasingly reporting cyber victimization and increasing in population, having exhibited the largest 10-year population growth between 2010 and 2020 to comprise about 16.8% of the U.S. population (Caplan, 2023; Caplan & Rabe, 2023), this study may also inform current law enforcement and cybersecurity efforts to reduce elderly victimization in the United States. Furthermore, the findings from this study may be of interest to other countries with similar aging population trends, especially many European countries with populations of more than 100,000 persons where the elderly comprise a larger share of the country's population (Caplan, 2023).

Finally, studying the mechanisms of learning and knowledge sharing in potentially criminally active darknet forums may help law enforcement agencies become aware of new criminal thought experiments and even detect novel attempts to make illegal activities appear less risky. For example, a recent study (Logie et al., 2023) found that buyers in a darknet marketplace were sharing harm reduction knowledge in the comment section of Adderall and Oxycodone listings. Another study (Steel, 2019) found that fraudsters are able to purchase victim data based on age and zip code, which allows for the identification of premium victims based on median income and home value. These studies demonstrate the exchange of knowledge among darknet users on matters of significance, as well as the collaborative efforts of niche groups to safeguard their community members as they devise methods to identify and exploit vulnerable groups they have identified as suitable targets.

2 | DATA AND METHODS

We use qualitative methods to examine the themes and content of Dread forum posts and comments from 2020 to 2023. This timeframe was selected given the documented increase in both digital/Internet activities and cyber-enabled fraud in the years following the pandemic. Based on our earlier observation that the elderly, as a subpopulation, may be an especially vulnerable victim population for cyber-enabled fraud, we followed a sampling strategy where we identified Dread forum discussions that included mentions of both fraud and the elderly. This strategy allowed us to increase the chances that the sample would offer insights related to the elderly subpopulation.

2.1 | Research questions

Our research broadly tries to answer the following research questions:

1. Why are Dread forum users planning fraud, especially against the elderly?
2. How are Dread forum users planning fraud, especially against the elderly?
3. How are Dread forum users creating and sharing criminogenic knowledge to plan fraud, especially against the elderly?

2.2 | Data collection

To collect data for this study, we used a web browser extension with a free and paid version. Through experimentation, Maras, Logie et al. (2023) concluded that the Tor browser is built on the Firefox core, which makes most Firefox add-ons and extensions accessible to the Tor browser. The advantage of utilizing a web browser extension, especially a paid version, is that it is updated and maintained by a knowledgeable third party, and social science researchers can easily implement this data collection method. For our data collection, we selected an extension capable of collecting data from all open tabs in a browser. Finally, the browser extension selected allowed users to save the webpages collected in multiple file formats.

Before starting the data collection process, we conducted a reconnaissance of the Dread forum. We first created a user account for the Dread forum. Although registration was not a prerequisite for accessing the forum, we found that the data collection process benefited from features reserved for registered user accounts. Once the forum was accessed using a registered account, we observed the layout of the forum, posts in subforums (subdreads), and comments on posts. We also observed the different subforums and the forum's search function. After utilizing the forum for several days, we decided to use the search function and several search terms to collect fraud-related data from the forum (see Table 1). The search terms selected were based on two criteria: (1) the term is used to describe an elderly individual, and (2) the term is used to describe fraud. We utilized Dreads search function to collect posts that included our search terms. The posts collected were retrieved from all subforums accessible to Dread's search function. Although there are subforums dedicated to fraud, we chose to collect posts from all available subforums. Using the fuzzy logic provided by the Dread forum search function, we added each search term and opened both the original post and original post for the comments the fuzzy logic search returned. Once all the results were accessed, we used the web browser add-in to collect and save the data as PDF files. This process was repeated for each search term.

TABLE 1 Search terms used to identify relevant forum post.

Use case	Terms
Search terms used in the data collection process	Defraud, Elderly, Elder, Embezzler, Government Agent, Grandparents, Hag, House Fraud, Investment scam, Lottery, Medical, Miracle Cure, No Spring Chicken, Old Timer, Patient Records, Pension, Romance Scam, Senile, Sextortion, Social Security, Sucker List Tech Support, W2, Warranty, Trust Fund, and Wire Fraud

2.3 | Data parsing and data coding

Once the data were collected, we created a program to perform data parsing and place the data collected in a database. We utilized a modified version of the Python parser program from Maras, Arsovska et al. (2023) to parse the data collected. The data collected were first converted to HTML using an Adobe script, which converted all PDF files into HTML files in a specified folder. The modified parser was then used to collect the original posts and comments. For each original post, the following data were collected and added to the database table "Original Post": name of the subforum, author of the post, title of the post, the content of the post, and the file the data were parsed from. Each comment was then added to the table "Post Comments" with the following data: name of the subforum, author of the comment, author of the original post, the original post content, and the file the comment was parsed from. After the data parsing process, 1037 original posts were added to the database, and 7365 comments on the original posts were added to the database.

Before starting the coding process, we performed basic data cleaning on the original post, primarily focusing on removing duplicate posts. Once this process was completed, the number of original posts was reduced to 969. We then coded three themes based on the following criteria: (1) "Elder-Specific" if it contained a reference to harming or using an elderly person while committing fraud, (2) "Opinion/Thought Experiment" when the post indicated that individuals were workshopping new methods or refining older methods while asking for community input, and (3) "Knowledge/Learning" if the author of the post was teaching or sharing knowledge, providing leads, or just providing general information on a method, victim, or service provider. Two reviewers coded these themes and also kept notes of terms that appeared to be important when describing different types of fraud, describing potential victims of fraud, and describing individuals with different job functions in the fraud ecosystem. Once the coders completed their independent coding of the Original Post data set, theme coding discrepancies were discussed and reconciled. We further refined our coding of specific fraud categories and excluded posts that were identified by the poster as a news article from our final data set. This resulted in 818 original posts being identified for further analysis and discussion. Apart from the three content themes described earlier, we created another theme called "Experience" to indicate posts where the user described the results of using particular methods or targeting specific victims, presumably based on previous experience or knowledge. This category due to the inclusion of perpetrators describing the steps in successful frauds allowed us to observe multiple stages of the fraud cycle and the differences that are unique to virtual spaces. The data were then coded for a list of cyber-enabled fraud categories selected by the researchers. This resulted in the identification of 10 fraud categories: (1) Payments/Bank/Credit Card, (2) Identity, (3) Mail Fraud, (4) Phishing/Data Hacking, (5) Real Estate, (6) Romance Scam/Sextortion, (7) Tax, (8) Tech Support, (9) Hate-motivated, and (10) Other fraud not meeting the criteria for any specific fraud category. Once this process was completed, we calculated an intercoder reliability score for the themes coded.

TABLE 2 Search terms used to identify relevant dread comments.

Use case	Terms
Terms used to identify relevant comments in the collected data	Defraud, Elderly, Elder, Embezzler, Government Agent, Grandparents, Hag, House Fraud, Investment scam, Lottery, Medical, Miracle Cure, No Spring Chicken, Old Timer, Patient Records, Pension, Romance Scam, Senile, Sextortion, Social Security, Sucker List Tech Support, W2, Warranty, Trust Fund, Wire Fraud, Credit Card, Check, Bank fraud, Sweepstakes, Inheritence, Confidence, Identity Theft, Phishing, personal info, Offline fraud, ATM, unemployment, Non-payment, Non-delivery, carding, drop, opsec, fullz, tutorials, mules, cashout, bill scam, payment, tax form, fraudscore, fraud score, bank log, banklog, pensioner, retirement, fabricated id, synthetic id, ginsengs, granny, grannies, grany, gift card, unemployment scam, cashing out, cash out, script, w-2, trustfund, sucker, miracle, grandparent, granparent, gran parent, grand parent, grand mother, grand father, papa, mama, mortgage, embezzle, embez, bank statement, romance, model, models, actor, actress, pharmac, store, dating, military, army, navy, marine, service member, veteran, patient, hospital, clinic, house, disable, coma, customer, healthcare, broke, abuse, rob, steal, swindle, social engineer, abandon, college, student, pay stub, paystub, insurance, extort, extortion, black mail, blackmail, pig butchering, payroll, pay roll, security fraud, tax evasion, tax, online shopping, bait and switch, bait \& switch, forge, forgery, charity, cheque, check, mail fraud, money laundering, embezzlement, advance fee, phishing, identity theft, widow, widows, old lady, old ladies, old man

We then modified the parser to identify comments that contained our original list of search terms and a new list of search terms identified after the completion of the theme-coding exercise of the Original Post data set (see Table 2). The parser identified 1365 comments containing at least one of the terms. These comments were then coded as related to the fraud method or the victim, perpetrator, or accessory to a fraud. Additionally, 480 comments were identified for further analysis. Many of the comments not meeting the coding criteria were located in subforums not dedicated to fraud. The results of our content analysis are presented in the following sections, with examples of posts, comments, and themes.

Finally, although the coders discussed the data coding to verify uniformity in the data coding and resolve issues, each coder first coded the data separately. Two coders reviewed the original post and coded the 818 posts with an intercoder reliability score of 0.965 using the Holsti method. The authors then checked the data to ensure no errors were present in the coded data.

2.4 | Plan of analysis

To answer our research questions, we first identified search words indicated by the FBI and our literature research to be associated with elderly fraud and used in posts in the context of fraud, with a further focus on posts that directly mentioned the elderly. We then examined themes in fraud and the most discussed fraud categories on forum posts. Additionally, we pay particular

attention to posts discussing the elderly. Finally, we analyzed the broad mechanisms, tools, and resources likely to drive learning through knowledge creation and sharing.

We utilized content analysis methods to explore our research questions and to highlight current or emerging themes of elderly fraud that were detected in Dread's darknet forum discussions. This follows guidance from earlier studies on darknet CoPs and knowledge-sharing networks, which typically recommend the content analysis approach for its ability to analyze, identify, and categorize the content of darknet forums such as activities, items, and tools (Sangher et al., 2023). Several darknet studies have utilized content analysis to understand themes and identify knowledge shared on marketplaces and forums (Bancroft, 2017; Logie et al., 2023; Maras, Arsovska et al., 2023; Maras et al., 2024). It is a common practice for studies to use social network analysis methods to understand the processes of learning, knowledge sharing, communication, trust, and reputation between members in hacking and darknet forums (Décary-Hétu & Dupont, 2012; Holt et al., 2012; Lu et al., 2010; Motoyama et al., 2011; Yue et al., 2019), and manual content analysis may be used either alone or as a precursor to social network analysis and other advanced methods of analysis such as automated topic modeling, document classification, sentiment analysis, and language modeling (Benjamin et al., 2019). The combination of manual content analysis and social network analysis was used by Maras, Logie et al. (2023) to identify the fentanyl network on the Alphabay marketplace. Although our study only utilizes manual and automated content analysis, we believe this is sufficient for identifying themes and key terms on the Dread forum.

3 | RESULTS

After coding our data set of 818 original posts, 573 posts met the criteria for at least involving fraud-specific discussion or one of our four themes of knowledge/learning, opinion/thought experiment, experience, or elder-specific post. The results of our coded data can be found in Table 3. Knowledge sharing/learning (44.1%) was the dominant theme in the data coded for all fraud categories except hate motivated. In comparison, the most common fraud type discussed is payments/bank/credit card fraud (25.1%). We further noted that approximately 50% of the payments/bank/credit card fraud discussions involved users describing their experiences. Finally, Thought Experiments (8.1%) involved fraudsters improving existing methods and creating new fraud schemes most notably by taking advantage of features in digital casinos and payment platforms.

3.1 | Research question 1: Why are Dread forum users planning fraud, especially against the elderly?

The findings suggest that the forum is highly favored among potential and veteran fraudsters, primarily due to its exceptional educational opportunities. This is especially beneficial for perpetrators who can easily find a wide array of low-risk targets through private sellers of exclusive data and receive valuable guidance and feedback from veteran fraudsters regarding untested techniques. Although our sample showed that the elderly were not exclusively targeted, they still emerged as a vulnerable demographic group, primarily due to the types of services offered to them and the risk of insider threats selling their data within a larger data set of vulnerable populations.

Scammers who favored targeting individuals more than 60 years of age perceived the elderly to be more susceptible to scams. Additionally, there were perpetrators who actively sought out

TABLE 3 Frequency/distribution (%) of themes for different fraud categories.

Fraud specifics	Fraud-specific posts (%)	Theme: Knowledge/learning (%)	Theme: Opinion/thought experiment (%)	Theme: Experience (%)	Theme: Elder-specific (%)
Any fraud type	77.1	44.1	8.1	18.6	2.7
Payments/bank/credit card	25.1	23.7	4.0	12.5	1.2
Identity	4.2	3.9	0.6	0.2	0.6
Mail fraud	2.1	2.0	0.2	0.7	0.0
Phishing/data hacking	4.0	3.6	0.2	0.4	0.1
Real estate	0.9	0.9	0.2	0.5	0.1
Romance scam/sextortion	2.2	2.1	0.4	1.1	0.0
Tax	0.7	0.7	0.6	0.5	0.2
Tech support	0.5	0.5	0.0	0.2	0.0
Hate-motivated	0.4	0.1	0.2	0.0	0.1
Other	37.2	6.7	1.5	2.4	0.2

Note: Themes are shown in columns and fraud categories in rows. Themes shown in this table are mutually exclusive of each other.

individuals older than 60, particularly those who have been previously scammed and were referred to as members of the "sucker list," signaling the likelihood that previously victimized elderly individuals are perceived as more susceptible to scams. Nevertheless, it should be noted that not all members of the forum upheld the moral value of victimizing the elderly. Some argued for a strict policy against individuals engaged in such behavior, whereas others mentioned a shift in their stance after witnessing the impact of elderly victimization on friends and family.

Our data contained discussions from many posts. In this section, we highlight some of the more interesting excerpts, categorized into several tables, that demonstrated the targeting of the elderly as one of many potential victim groups (see Table 4), as a specifically targeted victim group (see Table 5), and, surprisingly as potential accomplices (see Table 6).

Broadly, our analysis showed that perpetrators in the forum are likely to mention frauds that are both traditional and cyber enabled (see Tables 4 and 5). Our data also drew attention to targets that are especially vulnerable to data theft, showing that perpetrators are considering the level of a victim's vulnerability and risk exposure as a reason to target specific victim groups. In our observations of perpetrators targeting suitable victims with reduced risk of being caught, we observed that experienced Dread users also tend to share short guides about specific fraud methods and the measures one should take to minimize failure (see Table 5, Example 5). We also observed that the collection of the victim's identity can occur under the cover of a legitimate service offered to the victim by the perpetrator, following which the perpetrator then uses the victim's identity to make illegal purchases online of products and services using the victim's identity, credit card, and address data (see Table 5, Example 1). Elderly victims, including even those recently deceased, were viewed as particularly easy targets for identity theft; for instance, one fraudster, who claimed to be employed at a church, revealed their ability to obtain personal information of elderly and recently deceased victims through their job (see Table 5, Example 4). In Tables 7 and 8, the examples presented indirectly identify the elderly as targets based on demographic characteristics and

TABLE 4 Fraudsters targeting multiple subpopulations.

#	Relevant quotes from posts and comments
1	I was setting up one of these digital banking apps and I was amazed how they made it in a way that any nobody could get a credit card with such little effort. My idea go to people that have no account in any digital banking app (homeless people, boomers in rural areas) Pretend to be some authority that needs your info (Insert bullshit reason why I need your id, facial recognition) Create as many, digital bank accounts and get as much digital credit cards I could possibily have Get bitcoin/monero Or, if it works sell it in the darkweb what do you guys think? Is it possible?
2	I had a interesting idea while browsing amazon, specifically their newly launched prime wardrobe, where you choose up to 8 pieces of clothing. Amazon then sends you the clothing free of charge. you try it out, keep want you want and send the rest back. And amazon charges you only for what you kept. Now I noticed that amazon only accepts debt and credit cards atm for Prime Wardrobe, And for orders over 300 USD only credit. What if you purchased some stolen CC then you sign up for a new amazon account and choose a distant neighbors address as the shipping address. Then you proceed to load up with cashmere sweaters and shoes, basically the most expensive shit you can find then checkout with your new CC and ship. When it arrives, put on a hat and some sunglasses idk, go to the house where you shipped tell them you accidentally put down their address and they got your package. Then shut the account down and you should be in the clear? What do you guys think? Seems kinda risky using Stolen CCs, seems might get some fraud investigation involved, but my reasoning was Amazon wont really care or pursue something like this unless you do it more than a few times. I'm also not saying I am going to do this, just curious what you guys think
3	Tax fraud is a great way to earn a significant amount of money, with relatively low investment (compared to profit). You have probably come across tax/cash app sauce that has peeked your interest. No need to buy it, I'm gonna post the link in the comments. Bad news is that this specific method (filing it through the fuel credit via cash app) has been patched. Good news is that you can file taxes different way with same results. Another bad news is that this late in the year, a lot of (ppl) have already filled their taxes, so if you are using fullz/profiles, 90% of them will be rejected as already being filled. You can still get a good profit if you have enough resources, as once you get one successfully, you can cash out 20k. You have two types of cash app, first one is btc enabled, and second one is fully verified which means it has direct deposit enabled. The main difference regarding taxes is that if you don't have dd enabled you won't be able to receive the tax refund directly to the cash app. It is not a big problem, you can still go through the process, just on the end, there will be an option to choose how you want to receive funds. You have to choose to receive it on your bank account. Then add your bank drop routing and account number. You can get bank drop on the market for around $100 or less. TD bank worked great for me. Name on the bank account doesn't have to match victim name (it is not the case with all the banks). For the walkthrough on how to do taxes through cash app, watch the video linked at the bottom of the post. You need SSN, DOB, DL number with issue and exp date, address and non voip number. You can get a non voip phone number on phone blur. If you don't have DL number with issue and exp date you can use lookup service on the markets, they usually go for around $30. Pick the W-2 form and begin Use Best Buy EIN (Redacted) if you don't have employer info for your fullz Use a best buy location close to their home address Income Wages- 67k, federal withheld 28k, the rest blank Skip deductions Put you didn't file a tax return in 2021. You should get around 20k refund. After that, follow everything as showed in the video. There is a big chance that it will get rejected as person has already filed the taxes for this year. Just keep trying. Filling through cash app is good as it lowers the chances drastically for id.me verification, as cash app has their own verification. Bad side is that getting verified account is expensive when you factor in all the applications that will be rejected. You can file through Tax slayer, Turbotax or IRS website using the same method, it will be cheaper as you don't need a verified cash app account, only fullz.

TABLE 5 Fraudsters specifically targeting elderly victims.

#	Relevant quotes from posts and comments
1	I have no issue ripping people off on a day to day basis. This old fuck came into my store because apparently he lost his old phone and he wanted to file an insurance claim. I realized this old bastard was literally losing his mind. He didn't even know what a debit/credit card was. He saw it as a bank card which pissed me off even more for wasting my time. With a bit of slight of hand I snagged 2 cards while I helped him file the insurance claim. I must have opened up 3 amazon accounts trying to ship myself visa gift cards to pay by bills and this was with NO GUIDE WHATSOEVER!!! Just testing shit out and hoping for the best. In the end it ended up working on my phone but this was only after I accidentally shipped him a ps4 to his home address. Oh and I bought a few porn subscriptions too. The old man never knew what hit him. A few days later the gift cards came in and I used them to pay my bills and that's pretty much that. I've recently got back into the game and I figured I'd share some success story or whatever. To all the noobs out there… no one is going to help you. You have to help yourself
2	I am No great genuis, particularly with tech and fraud. And as for my age, well less days ahead then there are behind. Anyway, I have this older, past elderly friend. I am the closest and only person in my friend's life at 81 years old. My friend, whom is still totally independent, has been the target of a scammer recently. In fact, I just left the bank with him last week where he got a totally new acc/card phone/number/app update/email. It was really amazing to me what all happened, and since I have been here, always trying to education myself, it gave me some additional insight the social part of the fraud process. Of course, I said nothing of my activity here to anyone irl. For the past months my friend has been telling me about different odd things happening, mostly texts and emails that come appearing as bills and official looking efforts to help stop someone from stealing money from his bank account. My friend gets a retirement ss check. I have/had told my friend several times, Do Not respond to any of those emails or texts, that everything was fine with his money, etc. But I am not around all that much and obviously don't monitor his phone/computer activity. Finally, he calls frantic, telling me he has to have my bank account information to immediately transfer all his money out of his account, to prevent someone from stealing it, and proceeded to read me a list of charges already supposedly done. I dropped everything, went to get him and take him to the bank and show him the money was still there. At first he said: they said don't go to the bank because they are trying to track who is stealing the money. When we get to the bank and he sees that all the money is still there, just like it says in the mobile banking app, my friend proceeds to tell me and the bank that he thinks he might have given the scammer more info: Apparently he talked to the scammer for almost an hour, leading my friend to find the IP address of the phone, and whatever else goes along with that information that goes with that social-scamming process. At this point, I am hearing the bank manager say that he gave the scammer all the access he needs to transfer the money, but hasn't do so yet, and I am thinking WTF! Is that really the way this all works? I am thinking a couple other weird things and uncommon things have happened in my friend's life recently, that have both helped him become this target and that have occurred as a result, that just go along with this scam process. At least I was able to keep him from losing any money, as he really is just barely making it as it is. And I think he finally got to idea about how email and device verification works. So did I, for that matter.
3	Have drugs completely fucked your mind? Or do some of you not have a brain to begin with I saw someone here put a post saying he wants to order drugs to his grandmothers place with a fake SIM. Leave your poor grandmother out of your degenerate activities you scum.
4	I can get access to a recently deceased or an elderly person's info. I'm thinking about this option because I don't have the upfront capital to get someone to make an LLC for me yet. I figured I can set this up for a few months and then use the capital I get to ask someone to make a new LLC. So here goes Open up an account with the info I get File a church under a different name in New Mexico File the LLC under the name of the church. While I wait for paperwork or to clear I can make weekly deposits in the bank account I deploy my operation. I use slot apps to wash the money from the account. Alternatively, I could also send myself the money in the business bank account to the church, as tithes. I know there's plenty I need to improve on or flesh out, I'm open to any ideas.

(Continues)

TABLE 5 (Continued)

#	Relevant quotes from posts and comments
5	Hey Guys, Back With A Free Method For Amazon! For Any Questions PM ME! IF THIS POST REACHES 10 LIKES I WILL DROP MORE METHODS AMAZON VIDEO TUTORIAL! I Used A Local 72 Year Old Lady's Credit Card For Amazon: P haha Looked Up Her Addy And Drove To The Nearest Taco Bell, Less Than A Mile Away. I Then Added Her CC To My Amazon Account, Which Had 2 Previous Orders. I Browsed For About 10 Minutes, Then I Bought A 1/10th OZ Gold Coin With The Old Bitch's Credit Card. For The Shipping Address, I Made Sure To Use An Amazon Hub Locker In The Same Zipcode Of The Old Bitch. The Order Went Through, Shipped And I Got My Gold Coin. The Key For The Amazon Method To Work Is That The Shipping Zipcode Must Match The Billing Zipcode. This Means You Can Use Any CC, As Long As The Shipping Zipcode Matches The Billing Zipcode. Local Cards Work Best For This. For Anonymous Pickup, Use An Amazon Hub Locker In The Same Zipcode As The Card Holder. AGED AMAZON ACCOUNTS WITH ORDER HISTORY WORK THE BEST!
6	Hi yall just as a way to give back I would like to share a really profitable item that you should card next and that is golf clubs. Yes you heard that right. Now first I know what you'll say oh mate you've been doing fraud for 5 months you probably don't know anything. Trust me I know how to make bread legally and illegally I prefer to make it legally though. This is a way to give back to and share my knowledge. Most people trying a card electronics which is stupid sometimes because if you get a CC fullz with an elderly person chances are they aren't going to be buying a brand new Iphone 13 and the bank will see this. Golf is an elderly person's sport. I myself play and carded my golf set. Now I have done this 4 times with no issues I bought 10 cards 4 of which the victims were above 50 perfect for this to work. 2 of the victims were from Floridia and my main Drop is in Florida so taking this into consideration I could go big and buy a full golf set including Bag, Irons, Drivers, putter etc all with a value of 7k. I managed to spend 5,750 and 5000 and the cards and successfully got it sent to my drop and then shipped to my country which was $400 (I live in a isolated country). Once they got here I took them down to the pawn shop told him I played in two new year's tournaments and won both sets and sold them for 10k. All this happened within two weeks. Now the money isn't the best I mean 10k no one will turn that down but If you lived in the U.S or Europe you could make 100K a month doing this if you had access to your own CC's. Sites to card you may ask… just search up golf shops and brands around the victims location or country. hopefully you read this and took something out of it and try it next time you have a cc. I'm becoming a vendor next month just finalizing methods and guides
7	New scams are developing around the coronavirus outbreak. Individuals posing as police officers or bank officers demanding cards, pins, documents etc from elderly people in order to get their cash out for them as it won't be available over the lockdown period. Is anyone aware of any other Coronavirus related scams that are starting to unfold?
8	I have a few high balance bank accounts with everything I need (AN/RN, SSN, DOB, etc) only thing I don't have are the login details.. what's the best way to get into these accounts? is spamming the only way? if so how would I go about it these accounts are also owned by elderly ppl
9	Recently it happened to my grandparents and I saw how upset they were and I always used to say to myself it's okay because they get their money back and they did, but the distress it caused them was eye opening to me in a way that I never really considered

age-based services. Specifically, within Tables 7 and 8, several examples indicate an interest in individuals 60+, whereas other examples indicate an interest in data from Medicare and pension recipients. Additionally, perpetrators highlighted the attractiveness of elderly victims who lived in certain locations known to contain a large elderly population, as well as elderly victims who have previously fallen victims to frauds referring to them objectively as the "sucker list."

We also observed an unusual number of posts indicating that fraudsters desired the elderly as accomplices in primarily traditional fraud schemes. Although the original post provides valuable

TABLE 6 Elderly accomplices.

#	Relevant quotes from original posts and comments
1	Get cash get an older gentlemen to take it to a precious metals dealer turn 100k into gold and silver. This happens very often and is rarely a red flag. Take that untraceable gold and group it up into about 500k take it to a precious metals buyer and they will deposit it via a check into the old man's account. The man gives 20% to his or her kids and he puts you on his inheritance tax free money. So is this sketch cause if you have 50 grampas leaving you a 500k inheritance shit will get fishy.
2	Lets just do a thought experiment. Say you got a bunch of money in crypto because you know a lot of elderly that pay you in monero to mow their lawn, and it would look really suspicious if you deposited it all at once. Technically this is a serious crime, because you didn't pay any taxes for mowing Mr. Anderson's lawn that he paid you in Monero for… here's the thing though, you're not worried about paying taxes. You just want your money to look legit without anyone knowing it all came from you mowing Mr. Anderson's lawn, it would be quite embarrassing for you. So instead, you look at your artwork you have been drawing in your spare time, and decide, maybe this would fetch a good price from someone in the NFT market. So you get in touch with someone whose got NFT's and a lot of cash. They buy your NFT's for large amounts of money. You give them your monero in return, but pay the one who bought your NFT a certain percentage premium in return for making your money clear of any evidence that its money from Mr. Anderson. And in your taxes you report your income as being self employed as an artist? I know there's a lot more fined details in this whole process than I have mentioned. Things like the tax form you have to fill out specifically for self employment? Or is this considered self employment if your selling art? I need tech experts, crypto experts, and know hows in the realm of finance to help make this thought expiriment go further…
3	you could probably get away with it without the electronic prescription with a little social-engineering, especially in these times of covid send in an elderly person to pick it up, speak with a young/unexperienced looking clerk etc.
4	Don't think PO box will suffice, from what understand the address needs to be residential. In my community, people pay lower income elderly folks to utilize their mailbox (usually in an apt building).
5	Yeah, PO box doesn't work, vacant house doesn't really work, you want to do this for real? OK. you asked for it. Find a nice elderly person in your neighborhood. Maybe you're walking down the sidewalk when they're just getting home from the grocery store, and you offer to carry their bags in. Be charming and get them talking about what they like, the things that fill their day, feeding birds and the like. A few days later you drop in with some fresh baked cookies to talk a little more, and this time you notice the postman was just by and you ask if they'd like you to go fetch their mail for them. (By the way its important they have an actual mailbox not a slot in the door. I don't know what it's like in kiwiland but in the US most old people have mailboxes, idk). Anyway do this a 5-6 more times over the next month or so, and you should be getting to be good friends. No don't bring cookies every time. Maybe bring a brick of suet to hang in the yard for their birds, songbirds love that shit because its got wicked energy. Now obviously, to order large shipments of illegal drugs to their house, you're going to need to be fetching their mail for them every single day, so you're going to have to start dry-run that for a little while to make sure they don't get all queer on you about it. If they give you any heavy shit just say they remind you of your dear departed grandmama/papa and you've been kind of depressed since she/he died and it just brightens your day to stop in for a visit every day and, around mail time just happens to be when you're passing by on your way home from work and, etc. etc. Once they acclimate to this and it becomes routine then you're all set. Now obviously, if you're actually so paranoid that you find this necessary then its possible you're just not the kind of kind of person that's cut out for buying weight online from foreign countries (ideally, the kind of person who doesn';t really mind doing a 3-5 year bit if that's what it comes to). But who knows, maybe you like doing this kind of thing. Maybe the knowledge you made a sweet old person's life a little more colorful is enough for you, and the fact that no seized shipment will ever be connected to you is just icing on the cake. I don't know your life. People are fuckin nutty.
6	I've had an elderly lady hand my guy his weed pack in the US and asked if she could please borrow some if she let him use her address. Grannies are usually the fucking bomb peeps to get on your side if you want a drop close to home.

(Continues)

TABLE 6 (Continued)

#	Relevant quotes from original posts and comments
7	Get fullz, or find an elderly neighbor that needs help getting their mail. Otherwise you use a fullz to open PO box or mailbox at a local mail center; use covid mask and hat plus uber to get to the drop and get picked up/dropped off several blocks from home.
8	Find an elderly neighbor and strike up relationship where you bring in their mail everyday (or at least most days) for them. Set up ID for their address so you know when packs are coming (mostly) Boom! another drop.
9	Why go that route when you know the info is going to be hit 1 million times. Theres lists you can buy that are semi-sucker lists out there. I'm sure like people who buy swamp land or psychic consultations. We don't even know the scheme you're planning. If you're running with your own phone scheme then try by demographic first (OLD PEOPLE) and the type of list is important too. Don't know what angle your working (spoofing DEA/Customs/IRS?). But anyways there's enough tools out there to make the job easier dialers/list sorting/companies/spoofers/sims etc. What would worry me more is your payout method as its harder to cashout these days without a viable solution.
10	People who are in extreme distress over reversing a transaction with Visa, will be in extreme distress if their fishing pole gets knocked over. When I was doing fraud; carding, I typically would pull background reports/credit checks on the victims. If they're a 90-year-old woman with terminal brain cancer whose children are all dead, I won't mess with her. Just take the $10 loss.

insights into elderly fraud, the discussion on accomplices takes place in the comment sections of certain fraud-related posts (see Table 6). In the examples provided in Table 6, these comments provide insight into how the elderly are identified and recruited to be willing and unwilling accomplices. Many of the posters suggest that a number of elderly individuals may be willing to become accomplices in committing fraud that require minimal effort and involve minimal risk. This includes simply using their residential mailbox or address for delivery, selling precious metals, or using them to collect prescription medication at pharmacies. The example from the Dread forum discussions on the elderly as suitable targets existed on a spectrum and revealed interesting insights into forum members' attitudes regarding the purpose of targeting the elderly.

Finally, the content analysis also revealed that the forum as a platform offered some protective factors to counter elder-specific risks through posters indicating disagreement or moral opposition to exploiting the elderly. Not all members of the community approve of targeting elderly individuals, with one forum member expressing outrage at another member using his grandmother's home as a location for drug delivery without her consent (see Table 5, Example 3). One commenter even implied that they would have kicked out the poster had they been a moderator with the power to do so.

3.2 | Research question 2: How are Dread forum users planning fraud, especially against the elderly?

Dread posts provided insight into how fraudsters identify, group, and target fraud victims. A number of fraudsters indicated that background checks and credit checks offered insight into a victim and whether they would notice a fraudulent transaction. Fraudsters also appeared to value the feedback from members of the community to comment on schemes being developed to defraud victims in the future, in a manner best described as workshopping between the scheme's

TABLE 7 Data sources and requests for multiple victim subpopulations.

#	Relevant quotes from post and comments
1	We have data of the following:– Real Estate Investors– Stock and bond investors– Foreign investors– Disable– Allergy– Orthopedic– Arthritis– Senior Citizen– Diabetic– Tech Support– Sweeps—Health And many more. If you are interested in any of these or anyone not listed here
2	I have a few random questions regarding how I should start/what I should know in this field. I'm pretty knowledgeable with computers/privacy but when it comes to carding/fraud I know very little so I'd like any advise really. I currently work at an insurance company, I will not say what I do but I have access to PHI which includes SSN, DOB, ADDRESS, NAMES, INSURANCE, PHONE # and MEDICAL RECORDS. Does anyone know how much I can sell this information for? I wouldn't be able to get any physical documents just the information I have on screen.
3	I work in the health care profession (at a privately owned clinic) and have access to thousands of patient's information. Not just their medical records, but their ID, SS#, insurance Info, address, phone#, and answers to almost every security question when you think about since I know their parent's names/maiden names, hobbies, etc. I even have access to the MSR that the majority of patients use to pay with any card they choose (10% of patients use cash).The biggest issue I see is that the program only reveals the last 4 of the card when searching up a previous transaction. I can always say that the MSR is currently not working and manually type in the card information (which has happened a few times recently due to heavy rain messing with our internet connection). I know for all Visa cards the first 8 digits are 461O 4602. If the program saves the last 4 digits indefinitely then I just need to remember the 3rd set of digits, the expiration, and the cvv when manually typing it in. I'm really good at remembering long sequences of numbers/letters in a short period of time. Although the patient is staring at me while I do this it provides an additional security measure because they won't think I ran off somewhere and wrote down the details. I also have a co-worker who wants in and I have known them for 5+ years and trust them completely since I've met them way before we started working together. They can come up front during the checkout process and entertain the patient by promoting something on the front counter while I type in the information. This will allow the patient to still see I am just merely typing in their details although it will also help with attaching a positive memory to the end of an appointment making it harder for a patient to want to point fingers at us first. I often get quite close to patients and know what they do for a living and can even calculate when they get paid (since a lot of patients are either really open or because a lot of them work the same profession due to the area we are located in.)Additionally, there are 2 main types of patients we typically see. General medical patients usually pay anywhere from $15-$150. The aesthetic patients typically pay$250-$1k+. I know which patients are in a financially secure position and wouldn't notice anything missing for at least a few days. I would wait for a while to use the patient's info to lower suspicion. The goal is to have them use that card in as many transactions they can make at other retailers before I actually use the card so that they don't have an exact idea on how their info may have gotten stolen. Aesthetic patients usually come in once every 2-3 months so that could also help me out if I choose one of those patients since they don't come in weekly like most general medical patients. Is this an elaborate plan that could actually work? What are some flaws you see?
4	Don't forget about the hospital patient record dumps for sale. Lot of new information out there.

inventor and the forum members willing to debate the merits of the scheme while suggesting modifications.

Consistent with the concept of insider learners and other insiders who may directly sell data without being part of a criminal group (Allan, 2018), we noted the possibility of insider threats from lower level employees especially from organizations that are part of the health-care sector. One potential data seller was employed at a private clinic, and another employed at an insurance company, indicating their ability to obtain patient information (see Table 7, Examples 2 and 3). Additional data sellers were present in organizations that provided services to the elderly or were

TABLE 8 Elderly victims data sources and data requests.

1	First of all, I'm very new. I'm starting to learn to get some bread, and I'm not even sure about all the terms as everyone uses them but never explain, my guess is that they are in the guides. I'm gonna buy when I can. The thing is that by a relative's work, I have a ton of information on people, names, national ID, address, and even a picture of their ID on both sides that can be used, for example, to open a digital bank account. Obviously I can't use them now, as they can be very easily tracked down to me and my family. But my question is, will they be eventually usable? The project is over at the begging of next year and then the information should be eliminated, so if I keep them for a year or so they will not be related to my family's work anymore. On the other hand, there are some people that is very old and probably going to die soon. so, will they ever be useful and safe to use by me? I'm thinking long term, I wouldn't think of using them until the end of next year. Also, has anyone used information of dead people? You know, to open or verify accounts to use. cheers!
2	Looking for a patient list that provides the Medicare information for each patient Also interested if anyone has any experience with billing Medicare
3	I need lists of potential scam victims (60+ yo, pensioners, etc) with current contact info. If anyone could point me in the right direction I would appreciate it.
4	I am looking for a source that can provide hacked medical records of patients. I need to have access to their Medicare information as well as their fullz. Must be a large patient list from a medical office. Preferably from the state of Florida but I am still interested in other states as well
5	I have leads, but my source ran off to Mexico to avoid the feds. I need new ones as I'm just about out and finding more has been painstakingly difficult. I need people preferably aged 60 plus. IDC what they fell for could have been a Nigerian prince scheme or the Jamaican lottery; the crazier the better.

able to utilize their relationship with researchers, with one post mentioning access to elderly research data from a funded research project that was required to destroy the data at the end of the project (see Table 8).

The data also showed that even as perpetrators have a stronger preference to defraud the elderly using digital platforms, a small number of lone actors are willing to scam the elderly within the same geographic or physical location, using the victim's address to cover their own illegal activities. These perpetrators also tended to use delivery lockers and drop-off locations within the same zip code as the elderly victims, when utilizing their personal and banking information to make fraudulent purchases.

Although knowledge sharing is evident in numerous examples, some posts also offered fraudster perspectives from past experiences, which offered valuable insights into important fraud planning activities, practices, resources (including data), and potential mistakes and pitfalls. We examined several of these posts through the lens of the fraud cycle (Albrech et al., 2011). In Table 5, Example 1, the perpetrator utilized their position within a trusted organization to gather the victim's information and verify its authenticity by having access to an insurance claim and the victim's credit card. The perpetrator, however, did not conceal the creation of a new Amazon account, even accidentally shipping an item to the victim's address. During the Trial phase, the perpetrator engaged in second-dimensional actions such as buying gift cards, porn subscriptions, and a PlayStation 4, which are items within a specific price range. A successful Discovery phase is depicted in Example 2 of Table 5, although the subsequent action phase was obstructed and interrupted by external forces, preventing its execution. The perpetrator adopted the identity of a bank representative and employed social engineering tactics to convince the victim that they are protecting their funds from potential scammers. In this scenario, despite the absence of the described activity in the victim's banking app, the victim displayed more trust in the caller's words than the

information provided by the app. The specific distrust in technology during a phone call from an unknown individual creates a vulnerability that is arduous to mitigate solely through technological measures. In another example (see Table 5, Example 5), the perpetrator outlined the Action phase, employing the gathered information acquired during the discovery stage to formulate a cover-up. Additionally, they utilized an account with a purchase history and opted to utilize a delivery locker address located in the same vicinity as the victim. In this particular instance, the utilization of a delivery locker serves to obscure the fraud, reducing the likelihood of detection.

In another case, we observed a complete occurrence of a fraud cycle (see Table 3, Example 10). The perpetrator recounted their process of acquiring credit cards and then carefully selecting the cards to match their preferred victim demographic and geographic preferences to execute their fraud scheme. With full confidence in the method's success, the perpetrator purchased golf equipment valued at approximately $10,000, shipped the items internationally, and sold these items to a pawn store for approximately $10,000. The decision to purchase golf clubs was based on the belief that purchasing such a large item using an older victim's identity would attract less attention compared to buying expensive electronics. This example showed that the perpetrator acquired the credit card data and demographic information during the Discovery phase, followed by the Action phase, in which concealment was attempted by making purchases at stores located in the same state as the victim and then identifying drop-shipping locations within the same state. The reason for choosing these locations was to minimize the likelihood of the banking fraud system flagging the transaction as fraudulent and notifying the victim. In the Trial stage of this example, the perpetrator described testing the method using first-dimensional actions and making large purchases using second-dimensional cyber-enabled fraud actions that could be converted into cash.

Finally, certain posters solely focused on sharing knowledge and information related to the discovery phase, indicating that they sought targets that met highly specific criteria (see Table 8, Examples 2–5), which was different from typical Discovery stage activities that do not require such specificity. We can assume that the ability of these perpetrators to use software to extract or filter specific data may have led to this unexpected refinement in the Discovery stage.

3.3 | Research question 3: How are Dread forum users creating and sharing criminogenic knowledge to plan fraud, especially against the elderly?

Within the content of Dread posts and comments that we analyzed, acquiring guides like the darknet bible or a fraud bible was recommended to learn best practices. Both new and experienced users suggested thought experiments aimed at increasing the chance of success with current methods as well as discussing novel and emerging methods of monetizing victims' personal information and credit cards. Nonetheless, in order to gain insight into the manner in which users of the Dread forum generated, obtained, and propagated criminogenic knowledge, selected examples from the tables are examined through the lens of Allan's (2018) framework on Insider versus Outsider Alternative Pathways to Criminogenic Knowledge. The first observation from the examples provided in the tables from post and comments is that they would all be considered knowledge transmitted through darknet CoPs that served as alternative learning sources for users of the forum reading the post and comment. However, our examination is from the perspective of the posters to understand how the authors of the posts learned how to commit fraud and their positions as insiders or outsiders as defined by Allan.

First, Example 2 of Table 5 illustrates an external perpetrator who acquired the necessary information to carry out a successful wire transfer using a victim's details, including their IP address, from an individual who was at least an outsider-associate-victim. This can be achieved by using social engineering to extract specific data points from the victim needed to perform the wire transfer without triggering the bank's internal fraud system. This knowledge is known to lower level bank employees since the bank employee was able to explain how the information given to the perpetrator could be used to defraud the victim. Finally, it is unclear whether the perpetrator learned how to engage the customer from insider learning by being a former or current employee of a bank or using an alternative learning source such as darknet communities or guides, a criminal facilitator, or exposure to criminal investigation techniques or methods. When examining Example 1 of Table 5 within the context of Allan's framework, it is evident that the primary perpetrator is an individual within the organization who exploits their position as an internal learner to acquire the victim's identity and credit card details while providing a legitimate service. Although the perpetrator acquired the victim's information as an insider, they obtained the actual knowledge to commit the fraud from an unidentified alternative source, despite claiming not to have used a free or paid guide. However, judging by their current engagement with the darknet forum, it is most likely a result of their active participation in darknet CoPs.

Tables 7 and 8 provide examples where individual or organization targets are not identified. However, the individual selling the data has identified their relationship with the organization that is the source of the data. The individuals are not groups or outsiders who have infiltrated an organization's systems, rather they are insider threats who can be classified as internal learners (junior employees with access) offering data for sale on the forum (see Tables 7 and 8). This also differs from Allan's observation in which insiders and outsiders were members of organized crime groups. Instead, Tables 7 and 8 are lone actors who do not commit fraud themselves but instead use their insider access level to acquire and sell the data to forum members who use the data to commit frauds by learning their craft from traditional sources or alternative learning sources. The sector that is most represented in Tables 7 and 8 is the health-care sector, with religious and research organizations also appearing in the data set as susceptible to insider learner threats.

The evaluation of the previous examples, conducted through the application of two frameworks, highlights the importance of employing multiple frameworks to address cases that cannot be adequately dealt with by a single framework or frameworks that are unable to address every situation. Generally, the fraud cycle is particularly useful when identity theft is involved and the target is an individual rather than an organization. In addition, it is particularly useful when the items and purchases are known specifically the financial value of the services and the places the products and services are purchased from. Finally, Allan's insider outsider framework provides a method for understanding how the victim's data are obtained and how the perpetrator learns a particular fraud method. This method is particularly useful when the perpetrator provides insight into their position within an organization or where the data were taken. It is also useful when the perpetrator describes the steps taken to achieve the fraud successfully or how they learned or developed the fraud method.

Although the Dread forum data provided detailed descriptions for committing certain types of fraud, it did not provide personal information (fullz), credit card information, account information, or detailed guides (PDF or Word Documents) within the content of the subforums. We utilized Maras et al.'s (2019) darknet database to determine if purchasing some of the items described in post and comments was possible. Utilizing Alphabay, which was operational during our analysis timeframe, we found that many items described in the posts necessary to commit fraud were available for sale on Alphabay (see Table 9). The Alphabay listings showed that the

TABLE 9 Methods and data described in the dread forum and available for purchase.

Number of listings	Example listing on AlphaBay	Fraud type
2	ULTIMATE Amazon carding guide 2022	Carding
1	FULLZ LLC REAL EIN BUSINESS PROFILE WITH DOCUMENT PHOTOS	LLC Creation
12	A Simple Very Basic Guide On How To Make Bank Transfers	Wire Transfer
7	BUY ANON SIM CARDS OF THE WORLD	Tech Support
4	Medical Records Systems FULL database	Medical
6	crypto to cash	Wire Transfer
12	Fresh 100k Medicare data with DOB Medicare	Medicare
4	Real estate arbitrage scam method	Real Estate
2	Insurance Complete Database 250 M	Medical Billing

data, tools, and guides required to commit known and newer, less recognizable frauds are available for purchase on Alphabay. Additionally, we found multiple listings for most products and similar products were sold by multiple vendors. Estimating the number of Dread users learning from the platform is difficult given that (1) Dread allows unregistered users to read the post and comments on the platform and (2) users are able to buy tools and guides from alternative sources like Alphabay during this timeframe.

The results of study demonstrate the importance of utilizing multiple methods and frameworks when a single technique does not provide a complete picture of how fraud occurs, why specific victim groups are targeted, and the ways the perpetrator could obtain the knowledge required to commit the fraud. When applying multiple methods and frameworks to the data set, we gained more insight that would have been lost if one framework or method was used exclusively to examine the data. In the following sections, we discuss the implications of our findings and the limitations of our research methods.

4 | DISCUSSION

This study demonstrates the application of a learning-based framework, based on the concept of learning in virtual CoPs, and improves our understanding of how criminogenic learning may support the planning of fraud on darknet forums. We argue that it is broadly more advantageous from a law enforcement perspective to adopt a long-term "target to disrupt" strategy against criminally active darknet CoPs, using this learning-based methodological framework that cultivates a deeper understanding of "how" criminal actors on the darknet develop fraud plans throughout time and "why" they prefer certain targeting tactics. In addition, we offer important insights on how and why darknet users plan fraud to target the elderly, and these relate to the victims, offenders, methods, practices, and the data used to commit fraud.

First, consistent with our conceptualization of darknet forums as virtual CoPs with the shared practice of learning through discussion, collaboration, and knowledge sharing, we found themes of knowledge sharing in both posts and comments. We observed that our sample of Dread forum members sought and shared knowledge in various forms, including sharing of experiences, discussing thought experiments, requesting and providing leads to co-offend, expressing or seeking

leads to purchase data and skills, engaging in crime-as-a-service, and providing or seeking leads to source the latest guides and resources to self-learn how to plan fraud. These themes were observed for both general targeting and elder-specific targeting of fraud victimization.

Second, the forum discussions demonstrated the diversity of opinion and knowledge-sharing mechanisms related to committing fraud, for both victim targeting and elder-specific victim targeting. These discussions provided insight into who is a suitable target, why certain victims are viewed as desirable targets, how fraudsters view victims, especially elderly victims, and what learning materials or resources are held in high regard as important guides for fraud planning in the fraudster darknet community. Consistent with the assumptions of learning and knowledge sharing in darknet CoPs, we found several mentions and sales-like advertisements of fraud primers, how-to guides, and even personal training tutorials in the Dread subforums. These resources were relatively easy to locate. Many of these resources were clearly meant for newcomers to help them acquire and improve their fraud skills, making them of high interest for law enforcement to target.

In our analysis of fraud against the elderly, it was noteworthy that there were discussions about the use of traditional fraud methods, insider threats within organizations utilized by the elderly, and the recruitment of the elderly as accomplices. Some surprising findings included insider threats in organizations involving research, medical care, and insurance with access to elderly people's data. This demands special attention given concerns about insider threats and their ability to steal sensitive and personal information, which can be used in banking and payments fraud (Eric Cole, 2005; Homoliak et al., 2020; Randazzo, 2004; Wang et al., 2015). Yet another surprising finding related to how some fraudsters discussed elderly individuals as assets in committing tax fraud, medical billing fraud, and prescription fraud. Some others even appear to consider elderly victims' homes and mailboxes to be potential safe spaces to ship goods to, with or without their consent, leveraging the respectable age of the victims as a shield against detection of illegal or suspicious activities. Several authors of comments (in response to original posts) expressed their readiness to involve the elderly in fraud schemes, as unwilling or willing collaborators, was perhaps the most unexpected insight of this study. These insights largely upend the binary notion that fraudsters view the elderly either as targets who are either extremely vulnerable or as morally off-limits and highlight novel or indirect ways in which the elderly are made part of fraud plans either as victims or as accomplices. Much less surprising, and consistent with FBI advisories on common frauds against the elderly, was the finding that many fraudsters favored impersonation of authority figures as a tactic to get the elderly to hand over personal information to plan frauds related to banking and payments.

The act of committing fraud starts with the discovery phase, where knowledge sharing and transmission mechanisms are utilized to maximize the financial profits (Albrecht et al., 2011). Our study adds to fraud discovery literature by producing a list of important search words relevant to the detection of general fraud planning. Since we also included elder-specific keywords in our sampling method, this study further demonstrates how our framework of cyber-enabled fraud analysis can be modified to focus on specific fraud categories or specific victim categories, such as the elderly. In addition to the 24 key search words identified from the study's preliminary literature review, our content analysis of the Dread posts produced 121 additional terms that can be used to identify posts discussing elderly fraud. Although our study was limited to Dread, these terms tend to be universal and can therefore be replicated by other studies using the same or similar terms, suitably modified as per the specific topics of interest.

4.1 | Implications for policy and practice

Based on our overall findings, and consistent with other studies in the past, we recommend this method be considered as part of a larger structured strategy that begins with the identification of darknet forums of interest, which may factor in special victim populations, as our study does, or specific fraud categories. The exploratory content analysis demonstrated in our study may indicate trends in new and emerging crimes, which could then be used to refine key search words for more sophisticated methods such as topic modeling, social network analysis, and automated machine learning techniques to scale up the monitoring effort of darknet forums. Machine learning techniques, in particular, can greatly reduce the time required for such analysis while being able to handle more data from more forums and for longer periods of time, as seen in the case of Medicare fraud detection programs that have made use of large data sets analyzed by machine learning techniques (Herland et al., 2018; Johnson et al., 2019).

Based on some of the more specific insights from our study, we additionally present the following recommendations for law enforcement, policy makers, and practitioners:

1. Our study revealed that fraudsters on Dread considered the elderly as both victims and accomplices, with some utilizing their real-world elderly services and connections to learn about elderly cyber vulnerabilities. Although current advisories for the elderly are geared to educate potential victims, there may be some room to educate the elderly about the risks of becoming unwitting accomplices in fraud schemes or indirectly participating in other scams by lending residential addresses or identities.
2. Based on our sample of Dread forum posts between 2020 and 2023, we noted that most fraud-related discussions, including those specifically targeting the elderly, showed the highest preference for fraud schemes related to payments (bank checks, credit cards, digital payments, digital wallets, etc.), followed by identity theft with the intention to sell the data to other cybercriminals. Banks and financial institutions have taken the lead on educating their clients and customers about these consumer risks; however, it may require on-ground, community-based awareness campaigns to underline the seriously criminal nature of these fraud categories.
3. We found some mentions of insider threat in relation to the elderly subpopulation, arising from the risk of company employees stealing or sharing confidential customer information from sources such as hospital records, tax forms, and unemployment or disability benefits. Insider threats remain difficult to prevent because of the ability of insider employees to access records as part of occupational learning. There may, however, be potential for agencies like the FBI to utilize its IC3 data to warn frequently implicated hospitals and health-care services, tax services, and social services companies, including those maintained by government agencies, about the need to monitor systems for insider threat activities.
4. Our analysis also revealed some instances of online-to-offline fraud involving the post office, multi-fraud or unspecific fraud schemes, and transnational fraud perpetrators. Although federal law has given the FBI jurisdiction over computer and credit card fraud since the 1980s (Manky, 2013), greater clarity is needed on the topic of which federal agency would be in charge of enforcing newer and emerging categories of cybercrime. A report from the Department of Justice Office of the Inspector General (2020) highlighted key benefits for the FBI to establish "a coordinated FBI-wide dark web approach" with clear allocation of investigative responsibilities among operational units and clearer guidelines for darknet data collection and reporting (Department of Justice Office of the Inspector General, 2020, p. 1), which is a recommendation we concur with.

4.2 | Study limitations and future research

Our research focused primarily on the use of the fraud cycle and the alternative paths for criminogenic knowledge. We found that fraud discussions on Dread forums between 2020 and 2023 were dominated by themes of knowledge and experience sharing, which may potentially improve the quality of the discovery phase. Future research should examine the fraud cycle with the goal of determining the best entry point to first reduce the financial losses from fraud and second, reduce the success rate of fraudsters. This would make fraud unattractive by raising the cost to plan fraud.

Our study primarily identified cases that utilized a victim's identity to commit fraud. Beal's fraud taxonomy would be more suitable in comparison to the fraud cycle in research where the victim is either an organization or an individual, and the fraud involves a victim who is being defrauded by receiving a product or service willingly or unwillingly that is of inferior quality or nonexistent. Although it was not a goal of our study to examine taxonomic classifications of fraud, our content analysis indicates there is potential to develop a dynamic system of current and emerging fraud categorization that further lists subcategories of fraud ranked by number of mentions in darknet CoPs. This may be especially useful for law enforcement teams responsible for monitoring crime-planning trends in darknet CoPs. Our content analysis also revealed the presence of successful juvenile fraudsters as young as 14 on the forum. Juvenile fraudsters operating online and specifically on the darknet should be the subject of future fraud research, potentially even meriting its own category of fraud.

Finally, it is important to acknowledge the limitations of our study. First, our data come from a single darknet forum consisting of data generated during a 3-year period. Without analyzing other forums and timeframes, it is only possible to conclude that some fraudsters who used the Dread forum targeted victims in ways we have identified. Second, the forum is predominantly an English-speaking forum, and the results all used in this analysis were written in English. Finally, most forum users present themselves as lone actors or small groups (comprising two to five individuals). This demographic does not correspond to the larger non-English-speaking groups, which have been credited with many significant data breaches during the past decade.

In our study, we proposed a broad learning-based framework and methods to identify and target criminally active darknet CoPs, by generalizing findings from Dread discussions that occurred between 2020 and 2023 about fraud. We acknowledge the exploratory nature of our research and that further studies may be required to demonstrate the effectiveness of this approach. In addition, the findings from this study cannot be extended to a broader population without additional research. We also acknowledge certain sampling-based limitations of our study, specifically that we searched for Dread subforums that had at least one post related to the elderly for our reference time period, that is, between 2020 and 2023. As mentioned earlier, this was done with the intention of increasing our chances of identifying forums whose members are open to targeting elderly victims. However, our data analysis indicated that very few of the sampled original posts (2.7%) actually involved elder-specific discussion themes.

In conclusion, we argue that our approach, driven primarily by content analysis methods, can be easily replicated and may further be modified to focus on other potentially high-risk victim groups or other crime categories of interest. We further envision our content analysis method as a preliminary step to inform and optimize next steps, as part of a larger methodology to support practical efforts by law enforcement to disrupt the criminogenic learning pathway to cybercrime including cyber-enabled fraud. Although there is scope for further research using data from other darknet forums beyond Dread, this may be limited by darknet data availability itself.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

ORCID

Kenji Logie https://orcid.org/0000-0001-7107-6510
Sumita Das https://orcid.org/0000-0001-7256-8920

ENDNOTE

[1]Dread allows users to access the forum without being members; however, they are only allowed to observe and lack any ability to participate in forum activities.

REFERENCES

Akers, M. D., & Gissel, J. L. (2006). What is fraud and who is responsible? *Journal of Forensic Accounting*, *7*(1), 247–256.

Akers, R. L. (1973). *Deviant behavior: A social learning approach*. Wadsworth Pub. Co.

Akinladejo, O. H. (2007). Advance fee fraud: Trends and issues in the Caribbean. *Journal of Financial Crime*, *14*(3), 320–339. https://doi.org/10.1108/13590790710758512

Albrecht, C., Albrecht, C., & Tzafrir, S. (2011). How to protect and minimize consumer risk to identity theft. *Journal of Financial Crime*, *18*(4), 405–414. https://doi.org/10.1108/13590791111173722

Allan, D. M. (2018). Insiders versus outsiders—Alternative paths to criminogenic knowledge. In R. G. Smith (Ed.), *Organised crime research in Australia 2018* (pp. 35–49). Australian Institute of Criminology.

Auer, R., Frost, J., Lammer, T., Rice, T., & Wadsworth, A. (2020). *Inclusive payments for the post-pandemic world*. SUERF Policy Notes, 193.

Bachmann, I., Kaufhold, K., Lewis, S., & Gil de Zúñiga, H. (2010). News platform preference: Advancing the effects of age and media consumption on political participation. *International Journal of Internet Science*, *5*, 34–47.

Bancroft, A. (2017). Responsible use to responsible harm: Illicit drug use and peer harm reduction in a darknet cryptomarket. *Health, Risk & Society*, *19*(7–8), 336–350. https://doi.org/10.1080/13698575.2017.1415304

Beals, M., DeLiema, M., & Deevy, M. (2015). *Framework for a taxonomy of fraud*. Financial Fraud Research Center. https://www.finrafoundation.org/sites/finrafoundation/files/framework-taxonomy-fraud.pdf

Beals, M. E., Carr, D. C., Mottola, G. R., Deevy, M. J., & Carstensen, L. L. (2017). How does survey context impact self-reported fraud victimization? *The Gerontologist*, *57*(2), 329–340. https://doi.org/10.1093/geront/gnv082

Benjamin, V., Valacich, J. S., & Chen, H. (2019). DICE-E: A framework for conducting darknet identification, collection, evaluation with ethics. *Mis Quarterly*, *43*(1), 1–22.

Bermudez-Villalva, A., & Stringhini, G. (2021). The shady economy: Understanding the difference in trading activity from underground forums in different layers of the Web. *2021 APWG Symposium on Electronic Crime Research (ECrime)*, 1–10. https://doi.org/10.1109/ecrime54498.2021.9738751

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 974–2891.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims* (1st ed.). Routledge.

Buxton, J., & Bingham, T. (2015). The rise and challenge of dark net drug markets. *Policy Brief*, *7*(2), 1–24.

Calis, T., & Tsekouras, D. (2018). Multi-homing sellers and loyal buyers on darknet markets. https://api.semanticscholar.org/CorpusID:85539130

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social & Legal Studies*, *10*(2), 229–242. https://doi.org/10.1177/a017404

Caplan, Z. (2023, May 25). U.S. Older Population Grew From 2010 to 2020 at Fastest Rate Since 1880 to 1890. Census.Gov. https://www.census.gov/library/stories/2023/05/2020-census-united-states-older-population-grew.html

Caplan, Z., & Rabe, M. (2023). The Older Population: 2020. United States Census Bureau. https://www2.census.gov/library/publications/decennial/2020/census-briefs/c2020br-07.pdf

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, *2*(1), 26–38.

Chertoff, M., & Simon, T. (2015). The impact of the dark web on internet governance and cyber security. Centre for International Governance Innovation and Chatham House.

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308–333.
Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731.
Cisco. (2020). Cisco Annual Internet Report (2018–2023). Author.
Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589
Cole, T., & Miller, J. (2023). Do offenders [fraudsters] 'collaborate and listen'? A quantitative analysis of fraudsters' decision-making processes on active cybercrime marketplaces. *Journal of Victimology and Victim Justice*, *6*(1), 25–48. https://doi.org/10.1177/25166069221144793
Cross, C. (2017). 'But I've never sent them any personal details apart from my driver's licence number…': Exploring seniors' attitudes towards identity crime. *Security Journal*, *30*, 74–88.
Cross, C. (2021). Theorising the impact of COVID-19 on the fraud victimisation of older persons. *The Journal of Adult Protection*, *23*(2), 98–109.
Cross, C. (2022). Consumer fraud. In A. Harkness, J. Peterson, M. Bowden, C. Pedersen, & J. Donnermeyer (Eds.), *The encyclopedia of rural crime* (pp. 66–69). Bristol University Press. https://doi.org/10.56687/9781529222036-021
Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160–175.
DeLiema, M. (2018). Elder fraud and financial exploitation: Application of routine activity theory. *The Gerontologist*, *58*(4), 706–718.
Department of Justice Office of the Inspector General. (2020). *Audit of the Federal Bureau of Investigation's strategy and efforts to disrupt illegal dark web activities* (Audit Division Report 21-014). United States Department of Justice. https://oig.justice.gov/sites/default/files/reports/21-014.pdf
Diehl, T., Barnidge, M., & Gil De Zúñiga, H. (2019). Multi-platform news use and political participation across age groups: Toward a valid metric of platform diversity and its effects. *Journalism & Mass Communication Quarterly*, *96*(2), 428–451. https://doi.org/10.1177/1077699018783960
Duxbury, S. W., & Haynie, D. L. (2018). The network structure of opioid distribution on a darknet cryptomarket. *Journal of Quantitative Criminology*, *34*, 921–941.
Elueze, I., & Quan-Haase, A. (2018). Privacy attitudes and concerns in the digital lives of older adults: Westin's privacy attitude typology revisited. *American Behavioral Scientist*, *62*(10), 1372–1391.
Eric Cole, S. R. (2005). *Insider threat: Protecting the enterprise from sabotage, spying, and theft*. Elsevier Science. https://doi.org/10.1016/B978-1-59749-048-1.X5000-6
Federal Bureau of Investigation. (2024). *2023 Internet Crime Report*. Author.
Fenge, L.-A., & Lee, S. (2018). Understanding the risks of financial scams as part of elder abuse prevention. *The British Journal of Social Work*, *48*(4), 906–923. https://doi.org/10.1093/bjsw/bcy037
Fitzpatrick, M. J., & Hamill, S. B. (2010). Elder abuse: Factors related to perceptions of severity and likelihood of reporting. *Journal of Elder Abuse & Neglect*, *23*(1), 1–16. https://doi.org/10.1080/08946566.2011.534704
Fortune Business Insights. (2020). *Digital Payment Market Report #FBI101972*. Author.
Gillespie, A. A., & Magor, S. (2020). Tackling online fraud. *ERA Forum*, *20*, 439–454.
Gordin, N. G., Gomez, L. M., Pea, R. D., & Fishman, B. J. (1996). Using the World Wide Web to build learning communities in K-12. *Journal of Computer-Mediated Communication*, *2*(3). https://doi.org/10.1111/j.1083-6101.1996.tb00188.x
Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112–130. https://doi.org/10.1177/1362480614538645
Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243–249. https://doi.org/10.1177/a017405
Gu, Z. (2021). *Social support and help-seeking: When do elderly victims of consumer fraud notify authorities?* (Publication No. 28776467) [Master's thesis, University of Maryland]. ProQuest Dissertations & Theses Global. https://www.proquest.com/docview/2632785290/abstract/966C5B7101604ED4PQ/1
Hasham, S., Joshi, S., & Mikkelsen, D. (2019). *Financial crime and fraud in the age of cybersecurity*. McKinsey & Company.
Henri, F., & Pudelko, B. (2003). Understanding and analysing activity and learning in virtual communities. *Journal of Computer Assisted Learning*, *19*(4), 474–487. https://doi.org/10.1046/j.0266-4909.2003.00051.x

Herland, M., Khoshgoftaar, T. M., & Bauder, R. A. (2018). Big Data fraud detection using multiple medicare data sources. *Journal of Big Data*, *5*, Article 29. https://doi.org/10.1186/s40537-018-0138-3

Holm, E. (2017). The darknet: A new passageway to identity theft. *International Journal of Information Security and Cybercrime*, *6*(1), 41–50.

Holt, T. J. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime*, *14*(2–3), 155–174. https://doi.org/10.1080/17440572.2013.787925

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, *33*(2), 31–61. https://doi.org/10.1080/0735648X.2010.9721287

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81–103.

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology*, *6*(1), 891–903.

Holtfreter, K., Reisig, M. D., Pratt, T. C., & Holtfreter, R. E. (2015). Risky remote purchasing and identity theft victimization among older Internet users. *Psychology, Crime & Law*, *21*(7), 681–698.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2020). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys*, *52*(2), 1–40. https://doi.org/10.1145/3303771

Howell, C. J., Fisher, T., Muniz, C. N., Maimon, D., & Rotzinger, Y. (2023). A depiction and classification of the stolen data market ecosystem and comprising darknet markets: A multidisciplinary approach. *Journal of Contemporary Criminal Justice*, *39*(2), 298–317. https://doi.org/10.1177/10439862231158005

Huey, L., & Ferguson, L. (2022). *What do we know about senior citizens as cybervictims? A rapid evidence synthesis*. CrimRxiv. https://doi.org/10.21428/cb6ab371.e6b80803

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *The British Journal of Criminology*, *55*(3), 596–614. https://doi.org/10.1093/bjc/azu106

Internet Crime Complaint Center. (2024). *Federal Bureau of Investigation Elder Fraud Report 2023*. Author. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect*, *26*(2), 107–122.

Johnson, J. M., & Khoshgoftaar, T. M. (2019). Medicare fraud detection using neural networks. *Journal of Big Data*, *6*, Article 63. https://doi.org/10.1186/s40537-019-0225-0

Jordan, T., & Taylor, P. (2017). A sociology of hackers. In D. Wall (Ed.), *Cyberspace crime* (pp. 163–186). Routledge.

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, *26*(3), 293–312. https://doi.org/10.1007/s10610-020-09439-2

Kigerl, A. (2018). Profiling cybercriminals: Topic model clustering of carding forum member comment histories. *Social Science Computer Review*, *36*(5), 591–609. https://doi.org/10.1177/0894439317730296

Kwon, K. H., Yu, W., Kilar, S., Shao, C., Broussard, K., & Lutes, T. (2020). Knowledge sharing network in a community of illicit practice: A cybermarket subreddit case. *Proceedings of the 53rd Hawaii International Conference on System Sciences;* Maui, HI, USA; 7–10 January 2020.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology*, *57*(3), 704–722.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280.

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: Themes from UK research. *Crime, Law and Social Change*, *67*(1), 77–96. https://doi.org/10.1007/s10611-016-9648-0

Logie, K., Pugliese, K., & Acevedo, A. (2023). An examination of harm reduction strategies in Oxycodone and Adderall buyer feedback on AlphaBay. *Criminology & Public Policy*, *22*(4), 695–733. https://doi.org/10.1111/1745-9133.12652

Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social network analysis of a criminal hacker community. *The Journal of Computer Information Systems*, *51*(2), 31–41.

Manky, D. (2013). Cybercrime as a service: A very modern business. *Computer Fraud & Security*, *2013*(6), 9–13. https://doi.org/10.1016/S1361-3723(13)70053-8

Maras, M.-H., Arsovska, J., & Wandt, A. (2019). *Detecting fentanyl and major players in darknet drug markets by analyzing drug networks and developing a threat assessment tool*. U.S. Department of Justice, NIJ Research and Evaluation on Drugs and Crime FY 2019 (NIJ Award Number 2019-R2-CX-0018).

Maras, M.-H., Arsovska, J., Wandt, A. S., Knieps, M., & Logie, K. (2024). The SECI model and darknet markets: Knowledge creation in criminal organizations and communities of practice. *European Journal of Criminology*, *21*(2), 165–190. https://doi.org/10.1177/14773708221115167

Maras, M.-H., Arsovska, J., Wandt, A. S., & Logie, K. (2023). Keeping pace with the evolution of illicit darknet fentanyl markets: Using a mixed methods approach to identify trust signals and develop a vendor trustworthiness index. *Journal of Contemporary Criminal Justice*, *39*(2), 276–297. https://doi.org/10.1177/10439862231159530

Maras, M.-H., Logie, K., Arsovska, J., Wandt, A. S., & Barthuly, B. (2023). Decoding hidden darknet networks: What we learned about the illicit fentanyl trade on AlphaBay. *Journal of Forensic Sciences*, *68*(5), 1451–1469. https://doi.org/10.1111/1556-4029.15341

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381–410.

McGuire, M., & Dowling, S. (2013, October 7). *Cyber crime: A review of the evidence Research Report 75*. GOV.UK. https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Mears, D. P., Reisig, M. D., Scaggs, S., & Holtfreter, K. (2016). Efforts to reduce consumer fraud victimization among the elderly: The effect of information access on program awareness and contact. *Crime & Delinquency*, *62*(9), 1235–1259. https://doi.org/10.1177/0011128714555759

Mikhaylov, A., & Frank, R. (2016). Cards, money and two hacking forums: An analysis of online money laundering schemes. In J. Brynielsson & F. Johansson (Eds.), *2016 European Intelligence and Security Informatics Conference (EISIC)* (pp. 80–83). IEEE. https://doi.org/10.1109/EISIC.2016.021

Mirea, M., Wang, V., & Jung, J. (2019). The not so dark side of the darknet: A qualitative study. *Security Journal*, *32*, 102–118.

Morrison, B. A., Coventry, L., & Briggs, P. (2020). Technological change in the retirement transition and the implications for cybersecurity vulnerability in older adults. *Frontiers in Psychology*, *11*, Article 623. https://doi.org/10.3389/fpsyg.2020.00623

Morrison, B. A., Nicholson, J., Wood, B., & Briggs, P. (2023). Life after lockdown: The experiences of older adults in a contactless digital world. *Frontiers in Psychology*, *13*, Article 1100521. https://doi.org/10.3389/fpsyg.2022.1100521

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. In P. Thiran, & W. Willinger (Eds.), *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (pp. 71–80). Association for Computing Machinery.

Newman, G. R., & Clarke, R. V. (2013). *Superhighway robbery*. Routledge.

Nichani, M., & Hung, D. (2002). Can a community of practice exist online? *Educational Technology*, *42*(4), 49–54.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.

Nurse, J. R., & Bada, M. (2019). The group element of cybercrime: Types, dynamics, and criminal operations. In A. Attrill-Smith, C. Fullwood, M. Keep, & D. J. Kuss (Eds.), *The Oxford handbook of cyberpsychology* (pp. 691–715). Oxford University Press.

Parti, K. (2023). What is a capable guardian to older fraud victims? Comparison of younger and older victims' characteristics of online fraud utilizing routine activity theory. *Frontiers in Psychology*, *14*, Article 1118741.

Pete, I., Hughes, J., Chua, Y. T., & Bada, M. (2020). A social network analysis and comparison of six dark web forums. In L. O'Conner (Ed.), *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 484–493). IEEE.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296.

Randazzo, M. R., Michelle, K., Eileen, K., Dawn, C., & Andrew, M. (2004). *Insider threat study: Illicit cyber activity in the banking and finance sector*. United States Secret Service.

Rehman, T. U., Parveen, S., Usmani, M. A., & Khan, M. A. Y. (2023). Varieties and skills of cybercrime. *International Journal of Cyber Behavior, Psychology and Learning*, *13*(1), 1–13.

Rose, L. M. (2018). *Modernizing check fraud detection with machine learning* (Publication No. 13421455) [Doctoral dissertation, Utica College]. ProQuest Dissertations Publishing.

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science*, *9*(4), 427–442. https://doi.org/10.1177/1745691614535935

Sangher, K. S., Singh, A., Pandey, H. M., & Kumar, V. (2023). Towards safe cyber practices: Developing a proactive cyber-threat intelligence system for dark web forum content by identifying cybercrimes. *Information*, *14*(6), Article 349.

Shakarian, J., Gunn, A. T., & Shakarian, P. (2016). Exploring malicious hacker forums. In S. Jajodia, V. Subrahmanian, V. Swarup, & C. Wang (Eds.), *Cyber deception: Building the scientific foundation* (pp. 259–282). Springer.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, *15*(2–3), 111–129. https://doi.org/10.1007/s12117-012-9159-z

Steel, C. M. S. (2019). Stolen identity valuation and market evolution on the dark web. *International Journal of Cyber Criminology*, *13*(1), 70–83.

Sutherland, E. H. (1947). *Principles of criminology* (4th ed.). J. B. Lippincott Co.

Trentin, G. (2001). From formal training to communities of practice via network-based learning. *Educational Technology*, *41*(2), 5–14. http://www.jstor.org/stable/44428654

Vaisu, L., Warren, M., & Mackay, D. (2003). Defining fraud: Issues for organizations from an information systems perspective. In J. Hanisch, D. Falconer, S. Horrocks, & M. Hillier (Eds.), *Proceedings of the 7th Pacific Asia Conference on Information Systems* (pp. 971–979). University of South Australia.

van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115–127.

van Wilsem, J. (2013). 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168–178. https://doi.org/10.1093/esr/jcr053

Wasko, M. M., & Faraj, S. (2000). "It is what one does": Why people participate and help others in electronic communities of practice. *The Journal of Strategic Information Systems*, *9*(2-3), 155–173. https://doi.org/10.1016/S0963-8687(00)00045-7

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution. *MIS Quarterly*, *39*(1), 91–112.

Wang, Q.-H., Miller, S. M., & Deng, R. H. (2020). Driving cybersecurity policy insights from information on the internet. *IEEE Security & Privacy*, *18*(6), 42–50.

Wenger, E. (1998). Communities of practice: Learning as a social system. *Systems Thinker*, *9*(5), 2–3.

Weulen Kranenbarg, M. (2022). When do they offend together? Comparing co-offending between different types of cyber-offenses and traditional offenses. *Computers in Human Behavior*, *130*, Article 107186. https://doi.org/10.1016/j.chb.2022.107186

Weulen Kranenbarg, M., Ruiter, S., & Van Gelder, J.-L. (2021). Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders. *European Journal of Criminology*, *18*(3), 386–406. https://doi.org/10.1177/1477370819849677

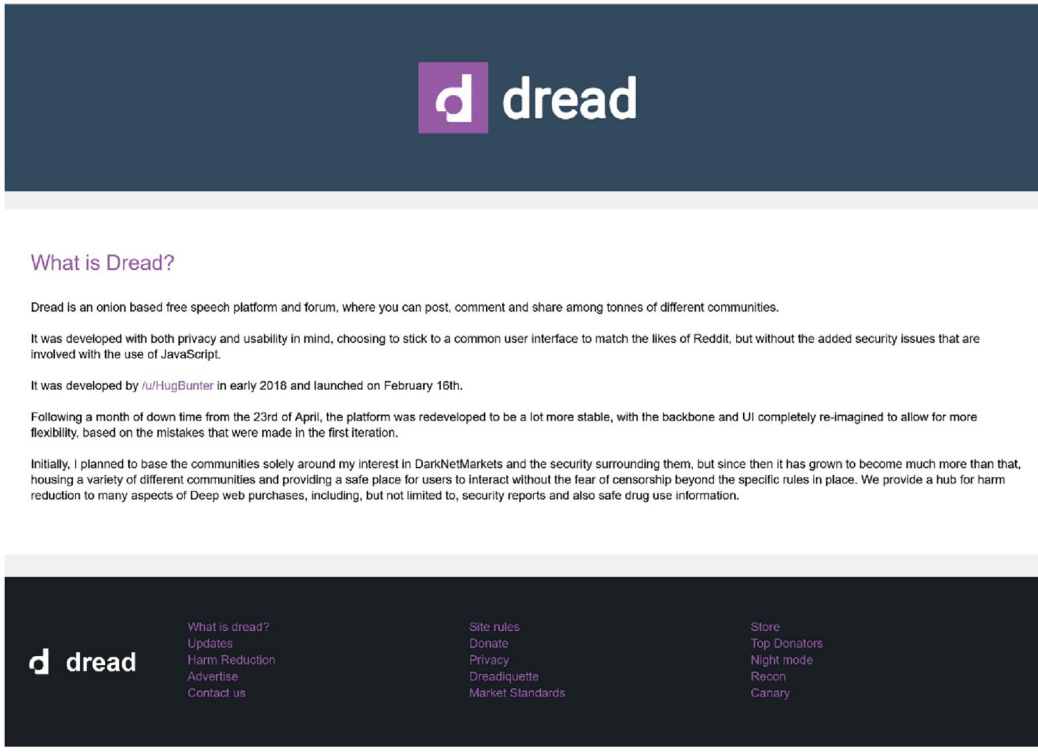
World Economic Forum. (2023). *The Global Risks Report 2023*. Author.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427.

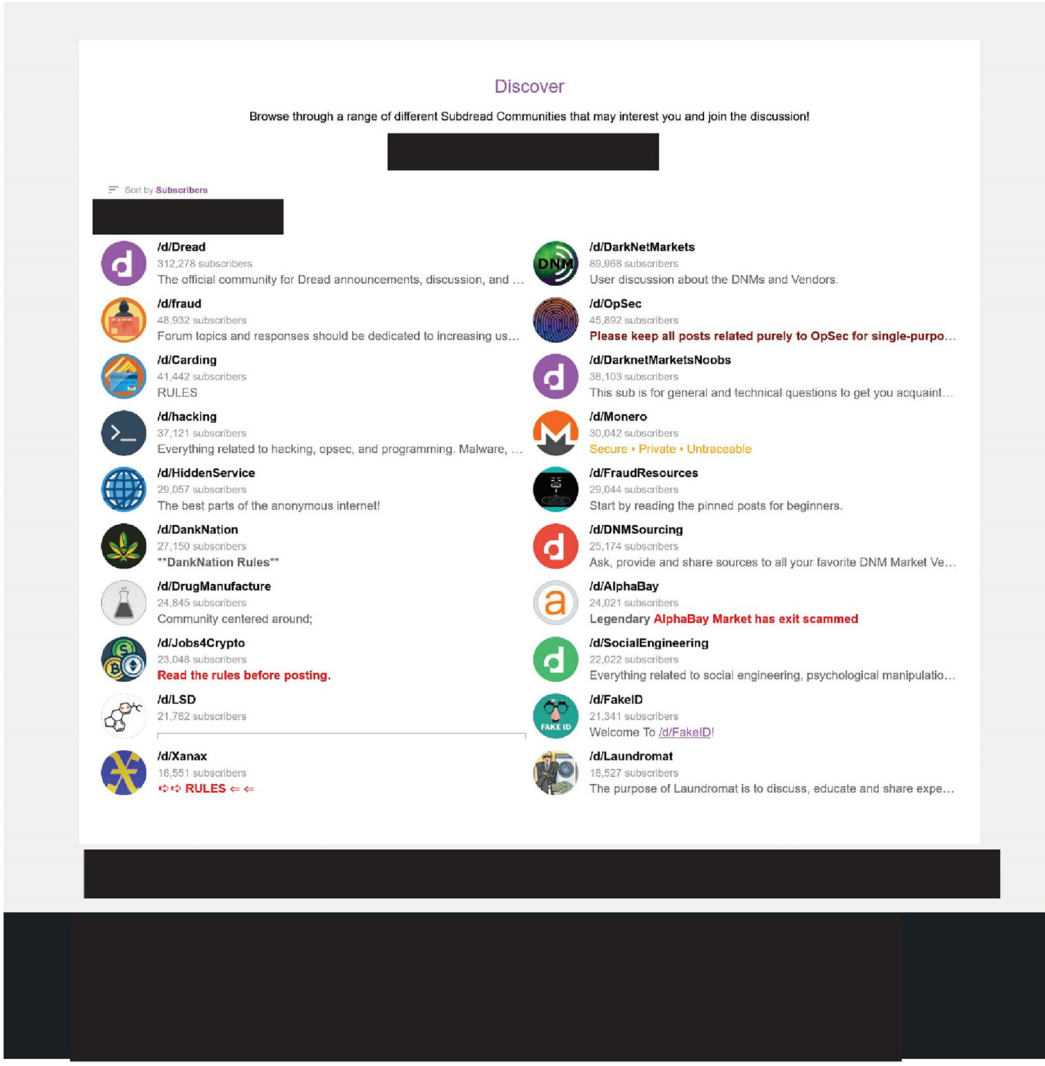
Yue, W. T., Wang, Q.-H., & Hui, K.-L. (2019). See no evil, hear no evil? Dissecting the impact of online hacker forums. *Mis Quarterly*, *43*(1), 73–95.

How to cite this article: Logie, K., & Das, S. (2025). Lessons learned from Dread darknet communities: How and why are fraudsters targeting the elderly to be victims or accomplices? *Criminology & Public Policy*, *24*, 237–271. https://doi.org/10.1111/1745-9133.12684

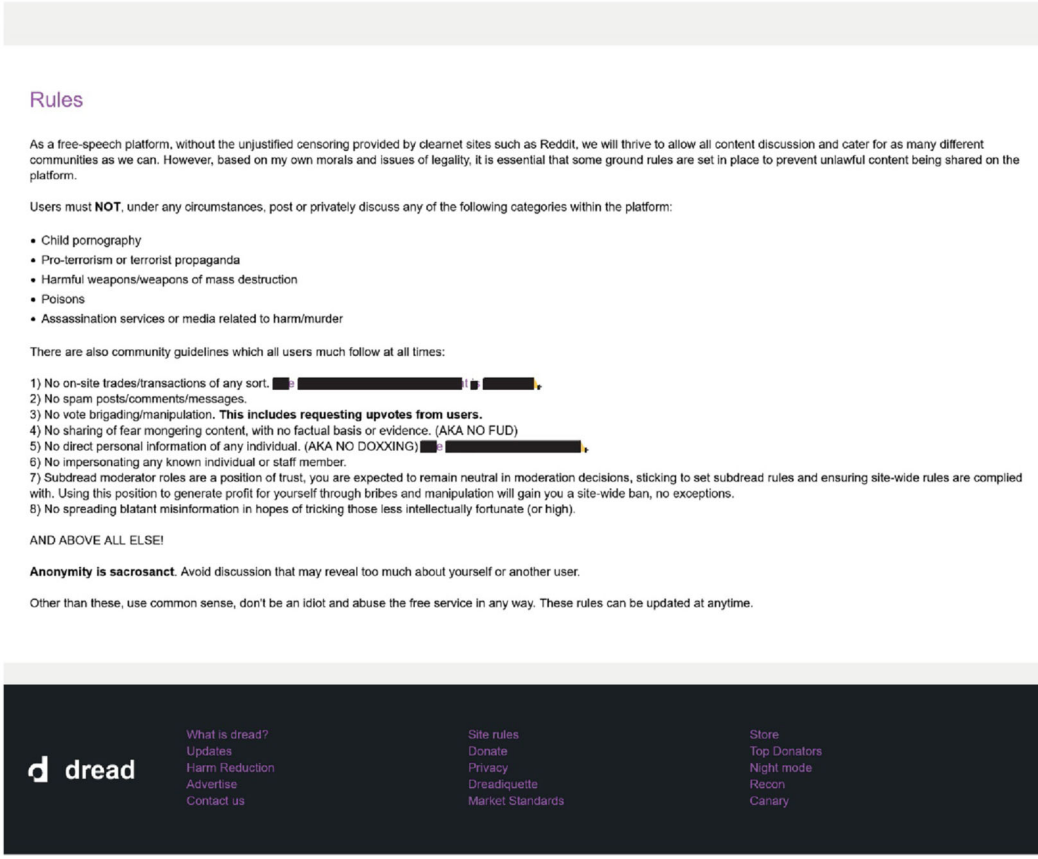
Appendix A: What is Dread



Appendix B: Top Dread Subforums



Appendix C: Dread Forum Rules



Rules

As a free-speech platform, without the unjustified censoring provided by clearnet sites such as Reddit, we will thrive to allow all content discussion and cater for as many different communities as we can. However, based on my own morals and issues of legality, it is essential that some ground rules are set in place to prevent unlawful content being shared on the platform.

Users must **NOT**, under any circumstances, post or privately discuss any of the following categories within the platform:

- Child pornography
- Pro-terrorism or terrorist propaganda
- Harmful weapons/weapons of mass destruction
- Poisons
- Assassination services or media related to harm/murder

There are also community guidelines which all users much follow at all times:

1) No on-site trades/transactions of any sort. [redacted]
2) No spam posts/comments/messages.
3) No vote brigading/manipulation. **This includes requesting upvotes from users.**
4) No sharing of fear mongering content, with no factual basis or evidence. (AKA NO FUD)
5) No direct personal information of any individual. (AKA NO DOXXING) [redacted]
6) No impersonating any known individual or staff member.
7) Subdread moderator roles are a position of trust, you are expected to remain neutral in moderation decisions, sticking to set subdread rules and ensuring site-wide rules are complied with. Using this position to generate profit for yourself through bribes and manipulation will gain you a site-wide ban, no exceptions.
8) No spreading blatant misinformation in hopes of tricking those less intellectually fortunate (or high).

AND ABOVE ALL ELSE!

Anonymity is sacrosanct. Avoid discussion that may reveal too much about yourself or another user.

Other than these, use common sense, don't be an idiot and abuse the free service in any way. These rules can be updated at anytime.

AUTHOR BIOGRAPHIES

Kenji Logie is a Ph.D. student in the Criminal Justice program at John Jay College of Criminal Justice and a research associate at the John Jay College of Criminal Justice Center for Cybercrime Studies. His research interests and publications include cybercrime, darknet forums, darknet marketplaces, and digital forensics.

Sumita Das is a mixed-methods researcher whose broad interests include security, crime prevention, and victimization. She holds an MA in Applied Quantitative Research from New York University and is currently pursuing a Ph.D. degree in Criminal Justice at John Jay College, City University of New York.