An empirical account of how scamming costs and life-stage influence desistance and recidivism among online scammers

Alain Claude Tambe Ebot
Paul H. Chook Department of
Information Systems and Statistics,
Baruch College, City University of New
York, USA
alainclaude.tambeebot@baruch.cuny.edu

Early-stage paper

ABSTRACT

Social engineering attacks such as Advance Fee Fraud (AFF) scamming and phishing are serious societal problems. Digital technologies are enabling scammers to produce newer and more sophisticated storylines for defrauding overseas buyers. Reports from consumer organizations and law enforcement agencies associate AFF scams with huge financial losses affecting millions of organizations and individuals yearly. As new technologies emerge, payment methods such as Zelle, CashApp, and gift cards make tracking and proving that a crime occurred challenging. Despite calls in several top journals for more active offender research in IS, research examining criminal desistance (the process of stopping criminal behavior) and criminal recidivism (the process of relapsing into a behavior following a period of abstention) among active offenders is mostly done by criminologists and sociologists. Following a preliminary analysis of interview data from online scammers, we identified (1) *scamming costs* as an overarching attribute for explaining scamming desistance and (2) *life-stage* as the core attribute for recidivism among online scammers. Our findings and contributions will demonstrate and highlight why IT and non-IT scamming costs influence recidivism and when they do not.

Keywords

Online scamming, AFF scamming, recidivism, desistance, deterrence, neutralization, social engineering.

INTRODUCTION

Social engineering attacks such as Advance Fee Fraud (AFF) scamming and phishing are serious societal problems (Tambe Ebot, Siponen, & Topalli, 2023). Reports from consumer

organizations and law enforcement agencies, such as the US FBI's Internet Crime Complaint Center (IC3) associate AFF scams with huge financial losses affecting millions of organizations and individuals yearly (e.g., see the FBI's, (IC3, 2022). The AFF scamming persuasion process involves multiple rounds of interactions with victims. Scammers use these interactions to provide evidence about their credibility and experience, deliver samples obtained through simple online searches, justify their locations, and suggest payment methods. Their overriding goal is to persuade victims into making multiple advance payments for nonexistent goods or services {Citation}(Burrell, 2008; Tambe Ebot & Siponen, 2014).

Notably, AFF scamming is not a single type of scam but an umbrella term for various scamming schemes including romance, investment, lottery, pet, drug, and employment scams (Action Fraud, 20223[1]; OCC, 2022)[2]. AFF scamming is also associated with many names in different countries. However, it is more commonly known as "419" scam or Nigerian "419" scams, a term coined after Section 419 of the Nigerian code criminalizing the offense. The Better Business Bureau's (BBB, 2022)[3] report revealed how pet scams alone cost US residents over $1 million USD in 2022 based largely on familiar storylines. For example, an individual who was relocating and needed a home for their puppy paid a rehoming fee of $250 USD through CashApp. After making the payment, the individual was surprised to learn she needed to pay an additional $80 USD. Another woman lost $850 USD for a Dalmatian puppy after visiting a pet website that looked "normal" (BBB, 2022). Moreover, as current technologies evolve while new ones emerge, payment methods such as Zelle and CashApp make tracking and proving that a crime occurred challenging because they allow users to electronically transfer money to anyone through email or a phone number. Recent evidence suggests that scammers prefer payment methods that bypass financial institutions, such as gift cards (Tambe Ebot et al. 2023).

Further, as scammers have unlimited access to search engines and social media platforms, they are very knowledgeable about the needs of individuals living in distant, overseas locations. In turn, such knowledge makes the scamming deception process more effective. Digital technology enables scammers to produce newer and more sophisticated storylines for defrauding overseas

[1] Advance fee fraud | Action Fraud
[2] Types of Consumer Fraud | OCC
[3] BBB Study Update: Average losses in puppy scams rising, even as cases fall

buyers. Prominent examples include pet and romance scams and more recently, drug scams. Crucially, advances in digital technology are associated with reduced risks and costs for online scammers. Given the financial rewards, anonymity, and convenience of conducting scams, online scammers are ignoring deterrence measures designed to curb their behaviors. Despite several calls for active offender research in IS, with a few exceptions (e.g., Tambe Ebot et al. 2023), such research is mostly done by criminologists and sociologists. However, scamming research from non-IS disciplines often overlooks the central role that information technology (IT) plays in online scammers' motivations.

The current study was initially designed to investigate the extent to which IS and non-IS attributes influence scamming desistance (the process of quitting online scamming) and scamming recidivism (i.e., the process of relapsing into scamming criminality). An initial analysis of the data indicates that online scammers are weighing the costs versus the benefits of scamming when deciding whether to desist or to reoffend. The preliminary findings also suggest that decisions to recidivate are overwhelmingly influenced by a core life-stage, a personal attribute. Consequently, we first refocused our research question to broadly recognize IT and non-IT scamming costs affecting scamming recidivism. Second, we examine why the effect of scamming costs on desistance is only temporary, leading to intermittent desisters.

RQ1: Why do scamming costs increase desistance among online scammers and when are they not effective?

RQ2: Why is the effect of scamming costs on scamming desistance only intermittent, leading desisted scammers to recidivate?

2. BACKGROUND

2.1. Scamming background

This section provides an overview of scamming, highlighting how traditional FtF scams emerged and transitioned into online scamming.

Traditional FtF scams

Although AFF scams are labeled differently across the globe, they are commonly known as Nigerian Prince scam, Nigerian 419 scams, or 419 scams. 419 is a reference to Section 419 of the Nigerian penal code criminalizing several fraudulent schemes (Adomi and Igun, 2008).

Currently, AFF scamming is an umbrella term for several variants of scams that deceive people into making advance payments to the scammers, irrespective of the context (i.e., physical FtF or online environments) (Tambe Ebot et al. 2023). Indeed, scholars have traced modern variations of AFF scams to the 16th century "Spanish Prisoner scam" (Smith, 2009), where scammers contacted businessmen through postal mail to invest money to smuggle a wealthy Spanish family member out of prison (Peel, 2006; Wood, 2014). While the businessmen were promised a share in the family's wealth, the deal was a fraud as there was no prisoner and no wealth was shared once the fee was paid. The origins of African scams have been traced to the 1980s when Nigerian scammers relied on postal mail and fax to transmit their handwritten letters (Cukier et al. 2008; Peel 2006). Historically, African scammers would deceive people during face-to-face (FtF) interactions. They would initially build credibility by appearing in expensive suits. In Cameroon, "men in suits" perform "black money scam" by promising to double victims' money (Ndjio, 2008). In the 1990s, Nigerian scammers evolved their letters to take advantage of internet communication resulting in an outpouring of AFF scam messages that either originated or purported to originate from Nigeria (Cukier et al., 2008). Notably, scamming letters were framed as official looking emails, sometimes about deceased senior Nigerian government officials who corruptly accrued large amounts of money.

Notably, online scammers create storylines that target people's greed by confirming stories they may have heard about Africa (Smith, 2010). Locally, the same phenomenon is practiced by fake charismatic pastors who urge their followers to make generous contributions in exchange for

God's riches to be manifested in wealth, marriage, or a visa to travel overseas. Earlier studies attributed the emergence and prevalence of AFF scamming to corruption and falling oil prices that caused the Nigerian economy to collapse (Peele 2005). Generally, scamming messages emphasize a prevailing problem from scammers' locality (e.g., poverty, corruption, witchcraft, or human rights abuse). Moreover, variations of AFF scams change over time as new scams emerge while existing ones fall out of fashion. In AFF scamming, any promises made by scammers, including wealth, merchandise (e.g., a puppy, drugs, or gold), services, assistance, and love, are contingent on the recipient making an upfront payment. Scammers will convince a victim that the purpose of the advance payments is to offset incidental expenses which can be cost of transportation, customs clearance, bank charges, money to setup a bank account, or flight tickets to meet a lover in romance scams (Akinladejo, 2007; Tambe Ebot e al. 2023). However, the advance fee request is a fraud because the scammer has no intention of fulfilling the promise.

Online scams

Although traditional FtF scams remain prevalent in the African countries often associated with online AFF scamming (Ndjio, 2008; Abia et al. 2010), the advent of digital technology has given scammers a global audience. Specifically, scamming attacks target Westerners because offenders assume they possess more disposable income. Before internet connectivity and smart devices were widespread and affordable, African scammers operated out of cybercafes. But continued improvements and affordability of digital technologies made it common for scammers to use mobile devices to practice scamming from anywhere. Indeed, the internet has transformed how AFF scams are committed, giving AFF scammers access to a worldwide audience. Nowadays, AFF scams evolve and adapt as technology improves; scamming messages are no longer based solely on million-dollar lottery wins, business propositions (e.g., investments), trunk boxes

containing gold, and Nigerian Prince stories (Ampratwum, 2009; Dion, 2010; Durkin & Brinkman, 2009; Holt & Graves, 2007). With access to search engines and social media platforms, scammers have a better perception of the needs of individuals living in distant, overseas locations. This is evident from the millions lost to scamming yearly. Thus, digital technology enables scammers to produce newer and more sophisticated storylines for defrauding overseas buyers.

In essence, online scammers are effectively exploiting platforms created for legitimate purposes to build lucrative but criminal enterprises (Whittaker and Button, 2020). Crucially, advances in digital technology are associated with reduced risks and costs for online scammers. Digital technologies have made online deception easier, faster, and more frequent, giving fraudsters access to an expanded pool of potential victims around the globe. For instance, whereas scammers previously relied on traditional financial institutions to receive advance payments from victims, technological advancements have presented newer and easier payment methods, including gift cards and bitcoins. In addition, scammers rely on their accomplices based in the US to collect payments made through Zelle or CashApp. Therefore, with affordances and possibilities from IT, scamming online as opposed to FtF scamming, offers scammers multiple levels of protection and scamming success, which in turn encourages scammers to persist in their criminality (Tambe Ebot et al. 2023).

2.2. Recidivism and desistance in online offending

This study investigates why and when scamming costs influence scamming desistance and why scammers who desist recidivate after some time. We note that several non-IT reasons explain persistent criminal behaviors for both FtF and online active offenders. Whereas online scamming is pervasive and consequential because of the digital environment, research suggests that the planning, design, development, and motivation for the crime occur in both the physical and

online environments (Tambe Ebot et al. 2023). Individuals who engage in online scamming initially learn and acquire proclivities (i.e., attitudes, motivations, and rationalizations) for committing and designing scams in the physical environment, making AFF scamming a hybrid crime. Criminological research suggests that in the FtF environment, factors that influence scamming offending include peer pressure, fun, and extravagant lifestyles (e.g., expenses to cover basic needs, clubbing, and luxurious consumer goods (De Haan & Vos 2003).

Further, many offenders eventually quit criminality for various reasons, a phenomenon known as desistance. In criminology, desistance is mostly viewed as a process of ending a period of involvement in crime (Farall et al.2005). Although some scholars have limited desistance to the final state of termination, the prevailing understanding is that desistance is a gradual process. This is because individuals who have been offenders from a young age are unlikely to suddenly cease offending completely (Bottoms, Shapland, Costello, Holmes, & Muir, 2004; Laub & Sampson, 2001; Maruna, 2001). For instance, Uggen and Kruttschnitt's (1998) definition of behavioral desistance implies a shift from a state of offending to one of nonoffending and its maintenance. Drawing insights from working with career criminals, Maruna (2001) noted that the definition of desistance needs to emphasize maintenance rather than termination because primary desistance occurs when habitual offenders spend time without offending. Fagan (1989) describes desistance as a process that occurs when the frequency (i.e., observed counts of offending behavior) and severity of the offending decreases.

While research suggests that most offenders desist from crime, research also finds that most criminals who desist from their criminality eventually reoffend, a process known as recidivism. For many years, the problem of recidivism has attracted the attention of criminologists. As early as 1917, researchers sought insights into the question of why some delinquents relapsed into crime while others did not (Buikhuisen and Hoekstra, 1974). Historically, offender recidivism was construed as a measure of individual or programmatic failure in the sense that either the offender refused to reform, or the punishment/treatment applied was ineffectual. Thus, recidivism studies have investigated factors such as biographical (age, education, profession, etc.) and judicial data (criminal record, age when first convicted, etc.); psychological traits (extraversion, neuroticism, intelligence, etc.) and psychiatric traits (psychopathy, schizophrenia, alcoholism, etc.); family factors (broken home, the atmosphere at home, etc.); school history

(achievement at school, disorderly behavior at school, truancy, etc.); work situation (unstable work history, unemployment, attitude towards work, etc.); and leisure activities (lack of interest and boredom) (Buikhuisen and Hoekstra, 1974). Recidivism as a measure of social failure highlights the extent to which lawbreakers in a society are not successfully reintegrated (Baumer et al. 2002).

Crucially, developments in technology are influencing recidivism research. In recent years, algorithms and artificial intelligence have attracted scholarly and journalistic attention. Algorithms and predictive analytics inform decisions in many sectors of public policy, including criminal justice. Of particular interest is the development of predictive technologies designed to estimate the likelihood of a future event, such as reoffending and recidivism. When judges, correctional authorities, and parole boards make decisions regarding incarceration, supervision, and prisoner release, they routinely rely on risk assessment instruments (RAIs), which serve as checklists for summarizing a persons' "risk factors" and estimating their likelihood of future reoffending. Some evidence suggests that RAIs outperform unaided human judgment when predicting recidivism (in Lin et al. 2020). Several studies found algorithms and RAIs to outperform the professional judgments of judges and correctional officers in predicting recidivism. However, a surprising finding by Dressel and Farid reported that human judgment was superior. With advances in machine learning and artificial intelligence, law enforcement agencies and courts in many countries are relying on algorithms. Although predictive algorithms are often carefully vetted for potential biases, it remains to be seen whether official crime records are a reliable source for determining recidivism (Kleinberg et al., 2019). Nevertheless, critics concerned that algorithms are racially biased against already disadvantaged groups oppose risk assessment instruments in criminal justice reforms.

2.3. Deterring online scamming

While the online environment is advantageous for offenders and reoffenders, it poses a significant difficulty for law enforcement efforts (Webster & Drew, 2017). Whereas scammers previously operated from poor and disadvantaged countries, digital technology has changed that. Technology enables scammers to spoof their locations and interact with victims around the clock without coming into physical contact with them (Button et al., 2014). Technologies that online criminals use to mask their locations and change their IP addresses are either freely available or

inexpensive to purchase. Search engines give offenders free access to a wealth of knowledge. Therefore, digital affordances allow previously disadvantaged individuals to effortlessly create anonymous or falsified identities while operating from anywhere (Webster & Drew, 2017). In several developed and developing countries, law enforcement efforts have introduced cyber-focused initiatives aimed at investigating and tackling this surge in online scamming attacks. For instance, the Australian government created the Australian Cyber Security Centre to encourage victims to file complaints. In the US, the FBI created a similar unit, the Internet Crime Complaint Center (IC3) for US residents. Several governmental and nongovernmental initiatives around the world have emerged to provide residents with a reporting mechanism for submitting complaints about how they were swindled by online scammers. Also notable are voluntary policing initiatives known as "digilanteism" that seek to track scammers, expose them, or at the very least, waste their time (Button, 2019, 2020).

Traditionally, deterring physical (face-to-face) and online criminal behaviors involve criminalizing them (Hui, Kim, & Wang, 2017) and many countries have instituted laws against AFF scamming and other cyber-offenses (Png et al. 2008; Hui, Kim, & Wang, 2017). However, as digital technologies enable offenders to mask their locations (e.g., using VPN or fake GPS) and benefit from anonymity, law enforcement efforts seeking to deter scammer activities are struggling to gather and link incriminating evidence against them. The transnational nature of online scamming attacks poses legal and logistical challenges to enforcement agencies. With the emergence of several social media sites, online criminals simply switch between platforms and their interactions with victims could be construed as legitimate business or personal interactions. While digital technology increases the effectiveness and efficiency of scamming, enforcement authorities in advanced countries find it challenging to identify, collect, and analyze digital evidence from cybercriminals (Holt, 2018; Hui, Kim, & Wang, 2017). Although local and transnational enforcement strategies against scammers have yielded some success, such enforcement strategies are ultimately ineffective in deterring cybercriminals (Holt, 2018; Popper, 2019). Further, it is not evident that deterrence measures against online scammers are successful.

3. METHODOLOGICAL APPROACHES

An important question in any research on offender decision-making is how they become offenders in the first place, and what factors encourage subsequent persistence of offending (see

Wright & Topalli, 2011; Sampson & Laub, 1995; Sampson, 2009). Previous IS research has examined the social learning process of becoming an online scammer (Tambe Ebot et al. 2023). By contrast, this study seeks to extend our understanding and knowledgebase of online scammers by investigating scammer recidivism. Specifically, we investigate when and how *scamming costs* influence recidivism among online scammers. In doing so, we aim to propose a theoretical model that identifies and explains the IT and non-IT scamming costs that affect recidivism among AFF scammers.

Consistent with many interpretive studies (Walsham, 1999), we did not approach this research problem with a theoretical perspective in mind. Further, our research problem has changed following our initial analysis of the data. This research-in-progress is based on data collected from online scammers operating in Cameroon, West Africa. At the time they were interviewed in 2021, some were active online scammers who had previously desisted or quit scamming criminality. So far, ten scammers have been interviewed and we intend to pursue more interviews. One scammer we interviewed returned into scamming on the day of the interview. Consistent with criminological literature, we construe the subjects for this study as intermittent desisters. We began the interviews by seeking to understand their reasons for quitting online scamming in the first place. We were also interested in what motivated them to reenter or what drives their intermittent behaviors. Following an initial analysis of the interview data, *scamming costs* emerged as the overarching attribute for understanding desistance among online scammers. This realization led us to reformulate our research question as follows: *RQ1: Why do scamming costs increase desistance among online scammers and when are they not effective?* However, it also emerged from the data that subjects had been moving in and out of scamming, a process known as intermittent desistance. This realization led us to also examine why the effects of scamming costs on desistance is only temporary. Thus, our second research question asks: *RQ2:*

Why is the effect of scamming costs on scamming desistance only intermittent, leading desisted scammers to recidivate?

The analysis of our preliminary analysis of the data alludes to several theoretical strands, including SLT, neutralization theory, and deterrence theory. However, as research on online scammers is limited, insights from our qualitative data will provide a more contextual, nuanced, and robust understanding of the IT and non-IT scamming costs that influence recidivism among online scammers. Therefore, we rely on existing theoretical frameworks as baseline scaffolding devices only.

3.1. Theoretical scaffolding

Research on recidivism and desistance are interrelated; to be a reoffender, the criminal must have desisted from crime, even for a short period. Typically, the planning, design, development, and motivation for online scamming take place in both the physical and online environments. Individuals who engage in online scamming initially learn and acquire proclivities (i.e., attitudes, motivations, and rationalizations) for committing and designing scams in the physical environment. Therefore, any study that addresses scamming reoffending or recidivism should incorporate attributes that influence scammers from the offline and online environments. Like information systems phenomena (Rai, 2018), research on desistance and recidivism from crime is dynamic with numerous theoretical perspectives competing and combining to explain it (see, for example, Sampson and Laub 1993; Warr 1998; Giordano et al. 2002). Examples of such theoretical strands range from social learning, neutralization, labeling, to deterrence. In the context of desistance and recidivism, criminologists note that no single theory that accounts for either phenomenon exists. This is not surprising since neither crime nor poverty is explained by a single theory (Maruna and Lebel, 2012).

For decades, several like-minded theories that focus on how people become criminals have addressed why people commit crime, desist from it, or reoffend (Clarke 1997). Examples include the life-course perspective, routine activity, deterrence, neutralization, labeling, social learning, strain, and rational choice. These theoretical strands have proven useful in IS security research (Moody, Siponen, & Pahnila, 2018) because they focus on the relationship between the offender and the environment in which the crime takes place.

The **life-course perspective** emphasizes how events that impact a person's life contribute to desistance from crime over time). The life-course perspective contends that salient life events (e.g., marriage, work, joining the military) may change criminal trajectories by affecting offenders' social bonds (Laub and Sampson, 2001). Accordingly, offenders desist because of a combination of individual and situational factors, some linked to important institutions. Life-course explanations contend that desistance is more than mere aging or "maturational reform" (Matza 1964); it is more like "turning points" or "epiphanies" because what it illuminates brings about a turning point in a person's life (Abbot, 1997; Denzin, 1989). Research suggests that desistance is associated with gaining employment; a job provides individuals with important social and economic resources (Meisenhelder, 1977) and generates a pattern of routine activities that conflicts and leaves individuals less time to engage in crime (Shover, 1983). But the evidence is also mixed. Regardless, the idea underlying the life-course perspective is that events in an offenders' life can lead them to "knife-off" from a lifetime of criminality.

Deterrence theory (DT) asserts that if an individual perceives the chances of being caught committing a crime as high (i.e., sanction certainty), the associated penalties as severe (i.e., sanction severity), and meted out quickly (i.e., sanction celerity), then the individual will be deterred from carrying out a criminal act (Nagin, 1998; Paternoster, 2010). In DT, certainty, severity, and celerity of punishment have a deterrence effect on offenders and would-be offenders; the threat of sanctions serves to force active offenders to desist from crime (Moody et al. 2018). The deterrence effect functions in two ways: First, through specific deterrence, where the prescribed punishment is designed to deter only the individual offender. Second, through general deterrence, where the punishment is designed to deter the general population from engaging in crime. The deterrence effect is often publicized to make potential offenders aware of the futility of participating in crime (Nagin, 1998; Tonry, 2008). Criminological reviews on deterrence theory have typically suggested that increases in punishment have overall marginal deterrence effects. However, the available evidence is also inconclusive, contested, and dependent on the specific crime (Tonry, 2008; Naggin, 1998). Although DT has been extensively studied (Nagin, 1998), research on deterrence has primarily focused on traditional crimes (Schell-Busey et al., 2016). Moreover, the effectiveness of deterrence measures is context dependent and influenced by offenders, how the crime is committed, informal factors (e.g., shame or fear of social stigma), and knowledge of the certainty, severity, and celerity of the

implementation of the measures. The existing evidence is also inconclusive. In some cases, deterrence is effective through informal sanctions, such as the fear of shame, for example, because offenders fear the social stigma (labeling—see labeling theory) of having a criminal record.

Further, offenders will undermine the impact of deterrence effects through neutralizing definitions (Siponen & Vance, 2010). Sykes and Matza's (1957) "**techniques of neutralization**" are justifications for engaging in criminal behavior. As a prelude to neutralization theory, Sykes and Matza (1957) leaned on Sutherland's differential association theory which posited that delinquency is a social behavior that is learned in the process of social interaction. The social learning process includes the techniques of committing crimes and the motives, drives, rationalizations, and attitudes that favor violating the law (Akers, 2017; Sutherland, 1947). To Sykes and Matza (1957), many criminals viewed offending as wrong from their upbringing because they share similar values and norms as other members of society and experience guilt and shame for their crimes.

Consequently, criminals can invoke defenses in the form of justifications to prove a lack of criminal intent. Even though these defenses of crime are not recognized by the legal system or society, criminals view them as justifiable. Therefore, they invoke them before committing a crime to absolve themselves from self-blame and neutralize the harmfulness of their criminality (Sykes & Matza, 1957). Thus, neutralization techniques are definitions conducive to crime because they allow would-be offenders to "neutralize" the illegality of crime before engaging in it. However, Sykes and Matza viewed neutralizations as a countervailing force to conventional values that are unimportant to delinquents.

FINDINGS

Table 1. summary of emerging findings

Core attribute	Desisting IT attributes	Desisting non-IT attributes
Scamming costs	**IT scamming costs that increase scamming desistance:** - Costs of blocking and blacklisting accounts - Costs of investments - Costs of apprehension	**Non-IT scamming costs that decrease desistance** - Costs to long-term goals - Costs of corruption from the local police - Cost of community rejection - Cost of the scamming lifestyle

		- Costs of justifications and neutralizations
Recidivism attributes: how personal and IT attributes increase recidivism among online scammers		
Personal attributes	Personal attributes that increase recidivism - Lack of a legitimate job - Family (marriage and children)	
IT attributes	IT attributes that increase recidivism - Scamming addiction - Ease and low cost of reentering online scamming - Gambling mindset	

Desisting or quitting IS attributes:

The findings here address why **IT scamming costs increase scamming desistance as well as when they do not increase desistance**. Our analysis identified two IT-enabled scamming costs that increase scamming desistance, namely***, costs of blocking and blacklisting accounts, cost of investments, and costs of apprehension***.

About a decade after most subjects became scammers, technological improvements have introduced some unavoidable scamming costs. *Costs of blocking and blacklisting accounts* emerge as social media sites relied on technology to block and ban accounts suspected of scamming more promptly than previously. Blocking an account is a huge cost to scammers because of its impact on relationships that scammers are grooming or fruitful transactions they are about to finalize. Subject 2 has been in and out of scamming and the day we interviewed him, he was making his return after a period of desistance. Here, he explains why he had desisted scamming for the second time:

I stopped again because I won the US lottery, but I didn't know that my name was on the scam alert list. That is the one that really broke me (the subject showed me his name on scam alert list. His name was uploaded in 2016 and he is listed on www.stop419scams.com for pet scamming in 2014). (Former scammer 2.1)

Even though scammers often undermine the effectiveness of the local police in apprehending them, the cost of being imprisoned for scamming hangs over them. Western countries are collaborating with African and other developing countries normally associated with scammer activity. Scammers typically associate Western law enforcement agencies with advanced technologies capable of tracking their whereabouts locally. While such concerns make them fearful of moving around with their smartphones, they need their smartphones to operate from anywhere at any time. Thus, when rumors spread that the US FBI was in Cameroon to cooperate with local law enforcement, scammers were worried. Scammers generally perceive and associate Western enforcement agencies with advanced technological capabilities:

We are worried that technological improvements make it easier for foreign police to catch us here. There was time last year (2020) when we heard the FBI was catching people in Yaounde. But by then I had also decided to quit, so I was ok. Otherwise, I would not be moving around with my phone. It is scary because law enforcement has come from Europe or America. But if it is just our local police officers, I don't worry about them. (Former scammer 2.1).

Cost of investments explains how the ease and increasing rate at which scamming accounts are blocked forced them to begin investing in protective technologies such as VPNs. Account blocking is not limited to social media platforms, such as Facebook but extends to ecommerce sites as well. For instance, Alibaba used to be a fertile place for scammers to post scamming adverts for nonexistent merchandise and receive replies from interested buyers without any problems. However, the pervasiveness of scamming on the platform led Alibaba to block all IP addresses originating from countries largely associated with scamming activity, including Cameroon. This means on one hand, scammers' accounts are easily blocked on social media sites; on another, they struggle to access some lucrative websites for posting scamming adverts. As a result, scammers require a VPN to overcome this preventive measure. Although free versions of VPNs are common and easy to download, scammers view the paid versions as more effective and reliable. However, this additional cost was unexpected yet unavoidable in terms of

scamming success. Crucially, most scammers cannot afford to invest in the paid versions of protective technologies, such as VPNs.

In terms of technology, as it improves, they easily block our accounts. Like I said, at first, you do a post on Alibaba for free and easily receive messages from interested buyers. But Alibaba blocked all IP addresses from Cameroon. It disturbed us. But then, we got the idea of using VPNs and there are different types of VPNs. As technology evolves, we invest money to buy services that can help us stay in scamming. (Former scammer 4.1)

When IT scamming costs do not increase scamming desistance

Although scamming costs encourage or motivate desistance, there are instances when their influence is limited. For instance, some subjects see the cost of investing in VPNs only as a necessary protective tool against being blocked from accessing certain websites. This means such investments did not motivate desistance. When asked whether he was worried that technological improvements would make apprehending scammers much easier, Subject 3.1 discussed VPNs as an effective anonymizing tool for bypassing websites that to block IP addresses from Cameroon.

I use VPN. I have a very strong VPN. It is the paid version. The free ones are not recommended. Mine is resistant to attacks. I got it through a friend in Canada (Former scammer 3.1).

A reason scammers may not view investments as conducive to desistance is that they avoid using their real identities online. Scammers can also invest money to buy identities from third parties. These are either missing identities or identities belonging to people who have died. Moreover, as technology evolves, new modes of receiving scamming money from overseas victims emerge. These new methods allow scammers to receive payments without revealing their real identities. Such developments also make blacklists effective only when the scammer is naïve about the possibility of being caught using their real identity. When subjects do not perceive blacklists as a

threat to their long-term goals, they also do not compute it as a high cost. Subjects 3.1 and 1.1 discussed the impact of scam alert lists on his life goals:

I hardly use my real name to receive money, so I am not afraid of scam alert lists. I go to the police station and buy missing ID cards and start using them (Former scammer 3.1).

I thought about its effect on my goals. I discovered that sometimes, a friend can send me money from the West, but I couldn't pick it up. I worried that I may want to go for a visa interview, and they discovered that I was a scammer. I didn't want to be blacklisted. But nowadays, there are other means of collecting money including mobile money (Former scammer 1.1)

Quitting non-IS attributes:

Why non-IT enabled scamming costs increase scamming desistance (or quitting)

The non-IT scamming costs that increase scamming include costs to long-term goals, cost of corruption, cost of community rejection, cost of scamming lifestyle, and costs of justifications and neutralizations.

Cost of scamming lifestyle and cost to long-term goals

The costs of long-term goals emerge because subjects became tired of making money through scamming only to spend it extravagantly within days. An important motivation in becoming a scammer is to make fast money and socialize with their scammer friends, often extravagantly. Subjects did not care about the excesses from their extravagant lifestyle because they "*they did not suffer to get the money*" (former Subject 1.1). But over time as scammers are aging, their perspectives have also been changing. They are becoming wary of spending long hours planning and orchestrating scams only to squander the money in a matter of days. Such concerns are particularly pronounced because subjects are thinking about investing in a legitimate venture. When asked how his desisting process unfolded, Subject 1.1 explained how at one point, he decided to quit for personal reasons:

Nothing happened to make me quit. I just decided to stop because I took scamming money, but I was doing anything tangible or real with it. The best I could do was chase girls, buy clothes and shoes, or go to nightclubs. I had a mindset to invest but I could not invest. I felt that because I did not suffer to get the money, I was just wasting it, so I decided to stop scamming. I was just excited by the scamming lifestyle when I joined it (Former scammer 1.1)

The **cost of corrupt police officers** is a symptom of the sociopolitical environment in which scammers operate. International bodies have consistently ranked Cameroon as among the most corrupt countries in the world. Scammers often pride themselves in their understanding of the needs of the local police and can address those needs. Corrupt police officers represented an expected cost that was easily met by giving them a cut from their criminal scamming proceeds. However, this cost emerged as a reason for desisting because of the excesses of these corrupt officers.

Costs of community rejection and reputation emerge from disapproval from scammers' neighborhoods. When they joined scamming as young adults attending university or as young boys attending middle or high school, subjects did not give credence to personal reputation. Their main goal was making money quickly to spend lavishly, often with loud bangs. Essentially, they desired to seen as heard; the process of making the money was irrelevant. This approach guided their behavior for many years. Scammers were just proud to be scammers and they enjoyed flaunting their ill-gotten wealth as a source of pride. But as they have grown older, intermittent desisters are realizing the downside risks from a bad reputation, the implications of being an outcast in your neighborhood, and the long-term effects from being blacklisted. For instance, Subject 5.1 specified that having a good reputation matters to date a girl from a "good" family.

Justifications and neutralization costs explain how scammers have become tired from deceiving themselves about their motives and dealing with complaints and cries from some

victims. Initially, making justifications and neutralizing scamming behavior was easy. The victims are overseas, most interactions are chat-based, and the idea that Westerners are wealthy and can afford to lose a few hundred dollars pervaded scamming communities. But as offenders interact and deceive victims, they became exposed to some victims' challenging situations. This mostly happened during pet scamming. Scammers have learned from experience that pet buyers are generally normal, law-abiding people seeking the animal for many personal reasons, including as a birthday gift to a child and as a companion. Justifying scamming such individuals wears down subjects over time. Scammers sometimes justify their criminality by blaming socioeconomic environment while casting themselves as victims to a corrupt system.

As well, using neutralizations has become a cost over time. Scammers invoke neutralizations to persist in their scamming criminality; they may claim that they are victims of a corrupt system or that they are poor and need money to survive. But most have come to realize that many of their victims are not wealthy either. To this, a scammer will argue that, but they are still better off because they are resident in a Western country.

When non-IT enabled scamming costs do not affect increase scamming desistance (or quitting)

CONCLUSION

This study is currently investigating two research problems pertinent to IS security:

RQ1: Why do scamming costs increase desistance among online scammers and when are they not effective?

RQ2: Why is the effect of scamming costs on scamming desistance only intermittent, leading desisted scammers to recidivate?

As we continue to develop this work-in-progress, we intend to conduct additional data collection from active online scammers who previously desisted.

REFERENCES

Akers, R. (2017). Social learning and social structure: A general theory of crime and deviance Routledge.

Akinladejo, O. H. 2007, "Advance Fee Fraud: Trends and Issues in the Caribbean," *Journal of Financial Crime* (14:3), pp. 320-339.

Alain Claude Tambe Ebot, Mikko Siponen & Volkan Topalli, 2023. "Towards a cybercontextual transmission model for online scamming", *European Journal of Information Systems* (forthcoming)

Ampratwum, E. F. 2009, "Advance Fee Fraud "419" and Investor Confidence in the Economies of SubSaharan African (SSA)," *Journal of Financial Crime* (16:1), pp. 67-79.

Abia, W. A., Jato, D. M., Agejo, P. A., Abia, E. A., Njuacha, G. E., Amana, D. A., ... & Ekuri, D. O. (2010). Cameroonian youths, their attractions to scamming and strategies to divert attention. *International NGO Journal*, *5*(5), 110-116.

Baumer, E. P., Wright, R., Kristinsdottir, K., & Gunnlaugsson, H. (2002). Crime, shame, and recidivism. The case of Iceland. *British Journal of Criminology*, *42*(1), 40-59.

Better Business Bureau. (2020). BBB warning: Puppy scam reports skyrocket during COVID-19 pandemic. Retrieved from https://www.bbb.org/article/news-releases/22363-is-that-quarantine-puppy-real-puppy-scam-reports-skyrocket-during-covid-19-pandemic-bbb-warns

Bottoms, A., Shapland, J., Costello, A., Holmes, D., & Muir, G. 2004. Towards desistance: Theoretical underpinnings for an empirical study. *The Howard Journal of Criminal Justice*, *43*(4), 368-389.

Burrell, J. 2008. Problematic empowerment: West african internet scams as strategic misrepresentation. Information Technologies & International Development, 4(4), pp. 15-30.

Brayne and Christin 2020. Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts

Buikhuisen, W., and H. A. Hoekstra. "Factors Related to Recidivism." *British Journal of Criminology*, vol. 14, no. 1, January 1974, pp. 63-69. HeinOnline.

Chang, J. J. 2008. An analysis of advance fee fraud on the internet. Journal of Financial Crime, 15(1), 71-81.

Chawki, M. 2009. Nigeria tackles advance fee fraud. Journal of Information, Law and Technology, 1(1), 1-20.

Chan, Jason, Shu He, Dandan Qiao, and Andrew B. Whinston. "Shedding Light on the Dark: The Impact of Legal Enforcement on Darknet Transactions." *Available at SSRN 3468426* (2019).

Carlsson 2013. Masculinities, persistence, and desistance

Clarke, Ronald V. 1997 "Problem-oriented policing and the potential contribution of criminology." *Report to the National Institute of Justice. Grant*.

Cukier, W., Ngwenyama, O. K., & Nesselroth-Woyzbun, E. J. 2008. Genres of spam. *Scandinavian Journal of Information Systems*, *20*(1), 1.

Denzin, N. K. 1989. *Interpretive biography* (Vol. 17). Sage.

De Haan, W., & Vos, J. 2003. A crying shame: The over-rationalized conception of man in the rational choice perspective. *Theoretical Criminology*, *7*(1), 29-54.

Farrall, S., & Calverley, A. 2005. *Understanding desistance from crime*. McGraw-Hill Education (UK).

Fagan, J. 1989. The social organization of drug use and drug dealing among urban gangs. *Criminology*, *27*(4), 633-670.

Giordano, P. C., Cernkovich, S. A., & Rudolph, J. L. 2002. Gender, crime, and desistance: Toward a theory of cognitive transformation. *American journal of sociology*, *107*(4), 990-1064.

Holt, Thomas J., George W. Burruss, and Adam M. Bossler. 2018. "Assessing the macro-level correlates of malware infections using a routine activities framework." *International journal of offender therapy and comparative criminology* 62, no. 6: 1720-1741.

Hui, Kai-Lung, Seung Hyun Kim, and Qiu-Hong Wang. 2017. "Cybercrime Deterrence and International Legislation." *Mis Quarterly* 41, no. 2: 497-524.

Lin et al. 2020. The limits of human predictions of recidivism

Laub, J. H., & Sampson, R. J. 2001. Understanding desistance from crime. *Crime and justice*, *28*, 1-69.

Lowry, P. B., Zhang, J., Wang, C., & Siponen, M. (2016). Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research*, *27*(4), 962-986

Maruna, S. 2004. Desistance from crime and explanatory style: A new direction in the psychology of reform. *Journal of Contemporary Criminal Justice*, *20*(2), 184-200.

Moody, G. D., Siponen, M., & Pahnila, S. 2018. Toward a unified model of information security policy compliance. *MIS quarterly*, *42*(1).

Meisenhelder, T. 1977. An exploratory study of exiting from criminal careers. *Criminology*, *15*(3), 319-334.

Nagin, Daniel S. 1998. "Criminal deterrence research at the outset of the twenty-first century." *Crime and justice* 23: 1-42.

Peel, M. 2006. Nigeria-related financial crime and its links with Britain. London: Chatham House.

Rai, A. 2018. Editor's comments: Beyond outdated labels: The blending of IS research traditions. *MIS Quarterly*, *42*(1), iii-vi.

Siponen, M., & Vance, A. 2010. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Smith, A. 2009. Nigerian scam e-mails and the charms of capital. *Cultural studies*, *23*(1), 27-47.

Schell-Busey, N., Simpson, S. S., Rorie, M., & Alper, M. 2016. What works? A systematic review of corporate crime deterrence. *Criminology & Public Policy*, *15*(2), 387-416.

Sykes, G. M., & Matza, D. 1957. Techniques of neutralization: A theory of delinquency. *American sociological review*, *22*(6), 664-670.

Tambe Ebot, A., 2023. Advance fee fraud scammers' criminal expertise and deceptive strategies: a qualitative case study. *Information & Computer Security*.

Topalli, V., & Wright, R. 2011. Dubs and Dees, Beats and Rims. *About Criminals: A View of the Offenders' World*, 50.

Uggen, C., & Kruttschnitt, C. 1998. Crime in the breaking: Gender differences in desistance. *Law & Soc'y Rev.*, *32*, 339.

Warr, M. 1998. Life-course transitions and desistance from crime. *Criminology*, *36*(2), 183-216.

Yar, M. 2005. The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427.