Author(s): Tambe, Ebot Alain Claude; Siponen, Mikko; Topalli, Volkan

Title: Towards a cybercontextual transmission model for online scamming

Year: 2023

Version: Accepted version (Final draft)

Please cite the original version:

Tambe, E. A. C., Siponen, M., & Topalli, V. (2023). Towards a cybercontextual transmission model for online scamming. European Journal of Information Systems, Early online. https://doi.org/10.1080/0960085x.2023.2210772

Alain C. Tambe Ebot[a], Mikko Siponen[b], Volkan Topalli[c]

[a]Paul H. Chook Department of Information Systems and Statistics, Zicklin School of Business, Baruch College, City University of New York, New York, NY, USA

[b]Faculty of Information Technology, University of Jyvaskyla, Finland

[c]The Andrew Young School of Policy Studies, Georgia State University

Towards a cybercontextual transmission model for online scamming

This study focuses on advance fee fraud (AFF) scamming, a specific form of online deception in which scammers rely on social engineering techniques to deceive individuals into making advance payments to them. Several industry and law enforcement reports have emphasised that AFF scamming is among the most pervasive forms of online social engineering attacks against consumers, organisations, and online users. Although AFF scamming has received significant attention worldwide, it remains an under-researched and poorly understood crime, and little work has focused on offenders. Although studies on online scammers have inferred that digital environment attributes influence online deception, few studies have empirically clarified how such contexts explain online scammers' motivations. The present study was designed to explore the motivations and deceptive practices of modern-day AFF scammers by using data from scammers. The empirical results urge the adoption of a model for AFF scamming that conceptually builds on social learning theory (SLT)'s core concepts but functions differently from it, warranting a new IT-based conceptual model. Accordingly, our contributions identify and explain cybercontextual social learning attributes that influence AFF scamming and underscore how traditional criminological theories, such as SLT, cannot sufficiently account for online offences, such as AFF scamming. Consequently, we propose cybercontextual transmission model (CTM) as a reformulation of SLT. Additional theory and practice implications are discussed.

Keywords: AFF scamming, social learning theory, qualitative research, inductive research, social engineering

Introduction

Advance fee fraud (AFF) scams are social engineering attacks where fraudsters take advantage of the online nature of digital communications to influence and manipulate individuals into making advance payments for non-existent merchandise (Tambe Ebot & Siponen, 2014). In AFF attacks, once scammers receive an initial advance payment, they are likely to make up new stories or recycle old ones to string victims along for additional advance fees until the victim discerns the scam and stops making payments. Various reports have identified AFF scamming and phishing as among the most pervasive forms of social engineering attacks (Internet Crime Complaint Center [IC3], 2019). Estimates suggest that, between January and August 2020, online scams cost consumers more than USD 100 million, representing an increase of over 12% from the previous year (ScamWatch, 2021). This uptick is further reflected in reports to law enforcement agencies worldwide. For example, in a 2020 annual report, the U.S. Federal Bureau of Investigation (FBI) IC3 estimated that costs from online advance fee–related scams (e.g., non-payment or non-delivery, advanced fees, misrepresentation, romance, investment, and charity scams) approximate USD 800 million (IC3, 2020). In addition, the U.S. Better Business Bureau (BBB) recently reported an increase of 24% in pet scams[1] (involving hard-to-acquire birds, puppies, or other exotic animals) in 2020 compared to 17% in 2019 (BBB, 2020). In fact, although 2020 saw an increase in AFF scam reports generally, pet scams skyrocketed during the Covid-19 pandemic, representing one of the largest recorded increases in online shopping fraud (BBB, 2020).

Notably, social engineering attacks, such as AFF scamming are being buoyed by the widespread prevalence of internet-based technologies (e.g., such as social media and mobile

[1] To illustrate, scammers offer pets on different social media platforms (typically for adoption), and the buyer needs to pay only the essential logistical costs associated with shipping the animal.

applications), giving fraudsters access to an expanded pool of potential victims around the globe. Although information systems (IS) scholars have made several calls in leading IS journals for studies that further our understanding of the motivations of cybercriminals (Benjamin et al., 2016; Ransbotham et al., 2016) or “black hat” offenders (Mahmood et al., 2010), research on offenders’ motivations is still emerging in the IS discipline (Benjamin et al., 2016; Ransbotham et al., 2016). Until recently, the extant scholarship on AFF mainly addressed these offences from the standpoint of victims (Button et al., 2014; Whittaker & Button, 2020; Wright et al., 2014), with a paucity of studies focusing on the offenders’ perspective. Furthermore, most theorising about offender motivation on AFF scams is concentrated on financial gain (Burrell, 2008), with the assumption that face-to-face (FtF) scamming and online scamming are equivalent crimes. This perspective overlooks the ways in which digital technologies foster cybercrime generally. Our review of the extant literature on AFF scamming attacks generally reveals that most studies infer or merely acknowledge in passing the influence of digital environments and processes on online deception. Fewer studies have empirically explained the extent of the involvement of digital IT in driving offenders’ decisions and behaviours. Thus, the present study first examines the extent to which the digital environment facilitates and motivates online offenders to engage and persist in AFF scamming.

Furthermore, given the lack of empirical scholarship on AFF scamming, we selected an inductive, qualitative approach (Walsham, 2006) based on interviews with active (i.e., non-institutionalised and currently offending) scammers. We began analysing the interviews inductively. However, it soon became apparent from the preliminary analysis that social and psychological definitions favourable to AFF scamming were being transmitted from more experienced AFF scammers to less experienced ones. This observation is reminiscent of Akers’

(1973, 2017) social learning theory (SLT), a well-known approach in criminology and IS that focuses on the transmission of skills and criminal beliefs between individuals that are critical to offending (Lowry et al., 2016). However, the subsequent analysis and comparison with SLT's core concepts revealed weaknesses in its assumptions regarding crimes taking place in IS contexts (i.e., online environment). Accordingly, the present study also examines the appropriateness of traditional social learning theories of crime for understanding and explaining online offending behaviours. There are two main take-aways from our work. First, the empirical results strongly urge the adoption of a model for AFF scamming that conceptually builds on SLT's core concepts but functionally differs from it, warranting a new IT-based model. Second, our findings emphasise the ways in which digital environmental attributes motivate and facilitate individuals to perpetrate online social engineering attacks. Consequently, our first contribution identifies and explains cybercontextual social learning attributes that influence engagement and persistence in AFF scamming. Meanwhile, our second contribution underscores how the SLT of crime, a traditional criminological theory, may either be wholly inappropriate for IS contexts or, as is the case with SLT, may need to be adapted to sufficiently account for online offences such as AFF scamming. To address this weakness, we propose a reformulation of SLT, which we call cybercontextual transmission model (CTM), for online social engineering offences like AFF scamming.

The remainder of this manuscript is organised as follows: First, we present a review of the literature on AFF scamming and social engineering attacks in IS and problematise our research problems. Second, we present Akers' SLT, of which our proposed CTM is a reformulation. Third, we discuss and justify the methodology used and present the interview findings. Fourth, we discuss the findings, contributions, implications, and limitations. Finally, we conclude the study.

Review of AFF scamming

We begin this section by providing an overview of AFF scams. We then briefly review AFF scamming in the behavioural IS security literature.

AFF scams

AFF scams have different labels worldwide. One popular name used in Cameroon is "feymania" as a reference to "feymen" (i.e., fake men) who promise to double victims' wealth. Local names in Ghana include "Sakawa" or Yahoo-yahoo" reflecting the role of search engines in scamming (Atta-Asamoah, 2009). More commonly, AFF scams are known as "Nigerian 419 scams" or "419 scams" after Section 419 of the Nigerian penal code criminalizing the offense. Crucially, scamming is not a recent development in economic crimes; AFF scams predate the internet and scholars have traced them to the sixteenth century "Spanish Prisoner scam" (Smith, 2009). In the Spanish Prisoner scam, scammers contacted businessmen through postal mail asking them to invest money to help smuggle a wealthy Spanish family member out of prison in exchange for a reward (Cukier et al., 2008). More recent expressions of AFF scams were traced to the 1980s when Nigerian criminals sent scam letters using postal mail to overseas victims (Cukier et al., 2008).

Traditionally, scamming letters were poorly written, and scammers would establish legitimacy by impersonating government officials or corporations. Typically, recipients were led to believe that they were lucky beneficiaries of millions of embezzled money. Thus, AFF scamming was perceived as a problem of greedy individuals who wanted to get rich quickly. In part, this explains the slow response by governments in the affected African countries (Akinladejo, 2007). Social scientists examining the socio-political roots of AFF scams from Africa attribute them to the social conditions that cause "…resource-rich states outside the Western world to fall into impoverishment, conflict and corruption" (Peel 2006 p. 2). Consequently, the prevalence of scamming in these countries is often attributed to poor socioeconomic performance, high unemployment rates, monetary rewards, poverty, mismanagement, corruption, and a lack of accountability and transparency (Akinladejo 2007; Ampratwum 2009; Burrell 2008). Research suggests that AFF messages from African scammers should be understood from a historical and social context (Bayart, 1999; Hibou, 1999), because they shed light on how scammers understand structural problems in their societies (Burrell, 2008; Smith, 2009). For instance, Smith (2009) reported that African scammers construct stories about postcolonial Africa to exploit shared beliefs (e.g., "stories you might have heard about Africa") in the West about Africans and Africa.

With the advent of digital technology, AFF scamming has metamorphosed into a global problem affecting individuals and businesses alike. Digital technology enables scammers to easily create and steal identities, download documents, copy "love quotes", and use webcam in live synchronous communications to meet victims' expectations (Burrell, 2008). Although online-based social engineering crimes, such as AFF scamming maintain many of the characteristics of FtF scamming, there are critical ways in which they function differently. In AFF attacks, once scammers receive an initial advance payment, they are likely to make up new stories or recycle old ones to string victims along for additional advance fees until the victim discerns the scam and stops making payments.

Estimates suggest that roughly one-third of security breaches in 2020 took advantage of social engineering tactics (Security Magazine, 2021). Scholars describe AFF scamming as a type of online fraud that leverages social engineering techniques to deceive individuals into making payments for non-existent merchandise (Burrell, 2008; Tambe Ebot & Siponen, 2014). AFF scamming is also an umbrella term for different scams that require advance payments for reasons that range from pets, employment opportunity, romance, lottery, and drugs to investments and romance (meeting a lover). Because our conceptual model is based on data from AFF offenders, it cannot yet be described as a “general” theory of fraud even though it contains characteristics that are assumed to be present in these different AFF scamming variations. However, this is also an empirical issue to be addressed in subsequent research. In some ways, the modus operandi of these variants or subcategories of AFF scamming are different; however, their shared goal involves deceiving individuals for financial gain. For instance, in pet and drug scamming, offenders employ social engineering techniques to manipulate and deceive individuals into making advance payments in exchange for merchandise that they neither possess nor intend to supply (Tambe Ebot & Siponen, 2014). Similarly, investment scams deceive people into committing funds to an “investment,” often through a purported investment broker, in exchange for a financial return (Lacey et al., 2020). Although scamming variants exploit different vulnerabilities, several academic and law enforcement reports suggest that a shared goal of AFF scammers is to receive financial payments (Jamieson et al., 2012; Webster & Drew, 2017; also, see Office of the Comptroller of the Currency, 2022 Queensland Police, 2022; StoneBridge, 2014; U.S. Securities and Exchange Commission, 2022). However, despite similarities in how variations of AFF scams apply social engineering techniques to manipulate victims, the scams may differ according to the fraudsters’ scamming script and backstory, in which each story determines the specific expectations of what action a victim is expected to perform. Reports suggest that scamming covers a wide range of behaviours, from unethical to criminal (Button & Cross, 2017). The IC3 (2019) has identified and defined at least 34 types of online scams.

The AFF scamming deception process typically involves multiple interactions between victims and offenders who employ deceptive techniques based on misrepresentation, document falsification, and deceptive declarations of empathy, love, or peril, depending on the AFF scamming variant (Abiola, 2009; Button et al., 2014; Whittaker & Button, 2020). In some of the most common scams, fraudsters place adverts of pets for sale or adoption, claiming that the animal is currently held somewhere less accessible or overseas. Following multiple interactions with an interested buyer, the fraudster requests an up-front payment to accommodate incidental costs (e.g., flights, vaccines, customs, or bribes for local officials) associated with transporting the merchandise (Tambe Ebot & Siponen, 2014). Table 1 in the appendix contains a brief overview of some AFF scams. It is far from exhaustive, particularly as new variants of scams emerge while existing ones disappear.

Problematising AFF scams in the behavioural IS security literature

To enable law enforcement and organisations to develop proactive cybersecurity capabilities that deter cyber-offenders, IS scholars maintain that it is necessary to understand cybercriminal behaviours (Benjamin et al., 2016; Mahmood et al., 2010). However, despite evidence that AFF scamming is one of the most pervasive social engineering attacks (IC3, 2019), relatively few papers have examined it. Some studies applied social psychological theories to understand scammers’ influence techniques of impersonation, urgency, and reciprocation (Chang, 2008; Whittaker & Button, 2020), and others have examined the economic impact of AFF scamming on investment, socio-political outcomes, and socioeconomic development in African and

Caribbean countries (Akinladejo, 2008; Ampratuwum, 2009; Boateng et al., 2008), finding an overall pervasive, negative impact across these measures (Burrell, 2008). This research also suggests that AFF messages from African scammers be understood from a historical and social context (Bayart, 1999; Hibou, 1999) because they shed light on how scammers understand structural problems (e.g., poverty, unemployment, and corruption) in their societies (Burrell, 2008; Smith, 2009). Smith (2009) reported that African scammers construct stories about postcolonial Africa to exploit shared beliefs (e.g., "stories you might have heard about Africa") in the West about Africans and Africa. For instance, such scammers may present themselves as naïve, ignorant, and desperate in some messages while claiming to be experts and legitimate suppliers of exotic animals in others (Tambe Ebot & Siponen, 2014). Table 2 presents a summary of AFF scamming studies and their findings.

A key research goal pertaining to offenders is to understand their motivation. Unsurprisingly, existing research suggests that scammers are primarily motivated by money (Abia et al., 2010; Burrell, 2008). This finding is hardly surprising, given that previous research has typically shown that scammers' tactics are influenced by their experiences of poverty, unemployment, corruption, and affordable internet access (Burrell, 2008). Such explanations are plausible yet inadequate, as many individuals who are poor, in need of money, and have internet access do not become criminals. Furthermore, our review of the behavioural IS security research on social engineering attacks suggests that with few exceptions (Burrell, 2008; Tade & Aliyu, 2011), scholars have mostly drawn on victims' accounts (Button & Cross, 2017; Whitty & Buchanan, 2016), secondary data acquired from international agencies (Ampratwum, 2009), or reviews of published articles that relied on secondary or anecdotal data (Abia et al., 2010; Duah & Kwabena, 2015). Whereas most social engineering studies have been approached from the perspective of victims (Whittaker & Button, 2020), studying why people are victimised via phishing messages cannot directly explain why offenders choose to victimise them in the first place. Thus, studies on victims provide only indirect and incomplete evidence regarding the motivations, tactics, and strategies of the offenders who take advantage of victims. Research in criminology suggests that the most accurate and insightful determinants of scammer motivations can be obtained only by asking offenders directly what they were feeling, thinking, and planning before, during, and after an offence (Topalli, Volkan, Dickinson, et al., 2020). Despite the aforementioned limitations in previous research, its contributions present interesting observations and opportunities for future social engineering–based research. First, with a few exceptions, the role of IT, the cyber-context, or the digital environment in the extant studies on AFF scamming mentioned above is often unclear. However, such knowledge may clarify our understanding of online scamming generally (and AFF scamming in particular) versus traditional FtF scamming. Traditional FtF scamming occurs in a physical environment where time, location, and appearance present constraints on scammers (e.g., a limited number of potential victims, fewer and slower communication modes, or barriers to anonymity). In the online world, however, many of these limitations are absent or rendered irrelevant with technology (Yar, 2005). Although previous studies on scamming have acknowledged or inferred that the digital environment influences cybercriminal motivations (Lowry et al., 2016), empirical explanations are rare. Consequently, little is known about the extent to which the digital environment promotes online scamming (and differentiates it from FtF scamming). The present study contributes to addressing this issue through the following research question (RQ1): How does the digital environment facilitate and motivate online offenders to engage and persist in AFF scamming?

Second, previous IS research on social engineering attacks and “black hat” offenders demonstrated that although IS scholars have applied criminological theories to understand them, our current knowledge of the motivations of active cyber-offenders in the IS literature remains largely anecdotal. Although SLT’s core concepts can adequately describe a process in which offenders learn to become scammers (i.e., the transmission of beliefs and attitudes from more to less experienced offenders; Akers, 2017), our preliminary data analysis revealed that it is inadequate for explaining offences that incorporate the transmission of beliefs and attitudes between online scammers in cyberenvironments. This observation led to our second research question focusing on the appropriateness of traditional social learning theories of crime for understanding and explaining offending behaviours online (RQ2): How can social learning theories of behaviour be reformulated to explain online scamming offences?

Background: an overview of Akers’ social learning theory (SLT)

In this section, we discuss SLT as a base theoretical framework. This study started inductively; therefore, our choice of theory (as well as its advantages and disadvantages for understanding AFF scamming) emerged only following a preliminary analysis of the interview data (see Section 4, where we explain how the methodology unfolded). The origins of SLT can be traced to the sociological behaviouristic approaches of sociologist and criminologist Edwin Sutherland (1947), with later modifications by psychologist Albert Bandura (e.g., see Bandura & McClelland, 1977). Their work stressed the reciprocal interaction between cognitive, social, and environmental factors (Bandura, 1977) in the human acquisition of attitudes, beliefs, and behaviours. In criminology, SLT in its current formulation has primarily been reformulated over several decades by Ronald Akers and colleagues (Akers, 2017; Akers et al., 2009; Burgess &

Akers, 1966), with important contributions by Cressey (1957), Sykes and Matza (1957), Hartung (1965), and Glaser (1956).

Akers' SLT emerged as an extension and reformation of Sutherland's (1947) differential association theory. It contends that delinquent peers influence rule-breaking through differential reinforcement and observational learning (Akers, 2017). SLT stresses that the process of learning about crime occurs through four central concepts: differential association (i.e., spending different amounts of time with different influencers in one's life), definitions (the value, rightness, or wrongness of criminal actions), imitations (the acquisition of behaviours and beliefs through various forms of observation), and differential reinforcement (the extent to which the outcomes of criminal or deviant choices are experienced as pleasurable or punishing; Akers et al., 2006). The theory posits that although differentially associating with criminals increases a person's likelihood of becoming an offender, mere association is not enough. Exposure must be frequent, intimate, and of extended duration. Furthermore, individuals are more likely to adopt ways of thinking and behaving from criminals when they see them as role models and observe them being rewarded for their law-breaking and deviance (a process referred to as vicarious reinforcement; see Bandura, 1977).

The developments of SLT have been influenced by the evolution of sociology and criminology, prompting the addition of a variety of concepts to improve the theory's descriptive and predictive accuracy (Burgess & Akers, 1966). These include the addition of social control variables and the incorporation of the cognitive concepts of learning and memory. For example, Akers integrated micro (social psychological) concepts of SLT with macro (sociological) concepts to propose an extension, social structure and social learning (SSSL) theory (Akers, 2017). Akers conceived of "social structure, culture, and locations" as rooted in a physical world.

However, SLT has yet to consider the specific characteristics of digital environments and processes as having their own effects on perception and behaviour.

For online offences, the traditional concepts associated with SLT, therefore, took on new meanings with new implications. For example, when Burgess and Akers reformulated differential association theory as SLT, they acknowledged television as an important new platform for socialising and learning delinquency (Burgess & Akers, 1966), recognising the potential for communication technologies to alter some of the basic processes underlying the functionality of social learning. It is not difficult to imagine a further extension of SLT resulting from the influence of digital environments (such as IT-based platforms) on the social learning of crime.

This last point is critical to our current argument, given the advent of online technologies as a new social context for the commission of scamming. Criminology has a long history of integrating concepts of offender, victim, and context (variously referred to in research as "setting" or "situation" or "prevailing social conditions") together for the purpose of developing theories and models of offending (Cohen & Felson, 1979; Miethe & Meier, 1994; Wikström, 2006). However, its historical grounding in sociological definitions of context leaves it ill-suited to properly characterise and empirically investigate online offences (Yar, 2005). With few exceptions, criminological research has mainly treated IT-based crime as functionally and structurally equivalent to traditional crime, thereby ignoring their differences (see Topalli & Nikolovska, 2020). However, although some processes of AFF scamming take place offline (e.g., socialisation with established scammers), many—especially those associated with deceiving users—occur online. For example, Lowry (2016) recently drew on SLT to examine how social media affects adult engagement in cyberbullying behaviours, reporting that internet attributes such as anonymity and scale distortion motivate offenders' decisions to choose cybercrime over physical crime.

Furthermore, SLT is a malleable theory. It has a history of adaptability and has undergone several reformulations. Thus, additional modifications of SLT are reasonable to expect as society adapts to the increasing integration of cyber and communications technologies into daily life. For more than six decades, sociologists and criminologists have been adapting SLT to clarify key concepts and constructs while ensuring that it accounts for micro- and macro-changes in the physical world (Burgess & Akers, 1966; Glaser, 1956). Incorporation of the online context is a logical extension. We provide a more detailed explanation of the core components of Akers' SLT in the appendix.

Methodology and the role of theory

This is an interpretive study (Klein & Myers, 1999) designed to understand how the digital environment facilitates and motivates offenders to engage in AFF scamming and how social learning theories can be reformulated to explain online scamming offences. In terms of theorising, the data collection began inductively in the sense that it was "as close as possible to the ideal of no theory under consideration." (Eisenhardt, 1989, p. 536). Subsequently, as the analysis of the emerging interview results showed some similarities with Akers' SLT, we adopted SLT as the baseline theoretical framework. This approach of using theory to further understand a phenomenon that began inductively is accepted and encouraged in the literature of inductive methodology (Eisenhardt, 1989), and IS scholars have variously labelled it "scaffolding," theory as a sensitising device (Klein & Myers, 1999; Sarker et al., 2018), and philosophically as abductive reasoning (Niiniluoto, 1999). Thus, as we openly coded the data (Urquhart, 2013) from our initial interviews with active AFF scammers, the analysis revealed a variety of behaviours and thinking consistent with the principles of SLT (see Akers, 2017). However, our choice of theory emerged and evolved over time before we subsequently employed SLT as a sensitising device (Walsham, 2006). Although SLT was initially relevant for understanding crimes that take place online, we later discovered that it could not explain some key observations of our findings, resulting in the need for future theory development. Because we used an iterative process that involved concurrently collecting and analysing data (Niemimaa & Niemimaa, 2019), the emerging theoretical narrative began appearing while additional data were being collected. Following the principle of overlapping analysis and data collection, we decided on analytical grounds where to sample from next (Urquhart, 2012; Walsham, 2006). Our empirical observations led us to more deeply and precisely pursue the emerging themes from our preliminary analysis in subsequent interviews with additional active offenders, further reifying our selection of SLT. At the same time, these more typical themes demonstrated the limitations of traditional SLT as an explanatory mechanism for how offenders learned about AFF scamming.

Methodological justification

To systematically understand why and how offenders (including AFF scammers) decide to engage in offending, it is necessary to access the knowledge that offenders have (Feeney, 1986). Doing so requires a rigorous qualitative approach that relies on semi-structured interviews, followed by coding and recoding transcribed data from offenders (Jacques, 2018). A rich history of this approach exists within the criminological literature (Topalli, Dickinson, & Jacques, 2020), and more recently, scholars have used it to investigate cybercriminals (Hutchings & Holt, 2018). In criminology, qualitative methods are preferred for examining how situational and dispositional factors influence crime and motivate offenders' decisions (Topalli et al., 2020). The qualitative method is also noted as a relevant tool in the development of theoretical concepts and frameworks (Urquhart, 2013).

Before we present our qualitative findings, it is important to comment on the internal validity of the interviews we conducted, and the possibility of distortion that might originate from interviewees' attempts to impress and deceive us, or dishonestly justify their conduct (Kirk et al., 1986; Liedtka, 1992). The prospect of distortion is not unique to this study; it is an issue that concerns all research based on offender interviews (Bernasco, 2013), where it is reasonable to suspect that interviewees may be less than forthright. To guard against deliberate dishonesty, we adopted an established methodological qualitative data collection regimen (Kirk et al., 1986; Topalli, 2005). For example, we carefully monitored all interviews, re-asked questions at various stages during the interviews to establish response congruence, and followed a detailed interview protocol, checking for and questioning inconsistent responses. Although this strategy does not eliminate the possibility of distortion, we take confidence in previous research showing that active offenders are no more likely than non-offenders to lie about their attitudes and behaviours (Jacobs et al., 2003). It should also be stressed that the same potential for dishonesty exists within all research formats in which participants are asked to discuss or report difficult or personal topics (Bernasco, 2013). Beyond that, the internal validity of these kinds of data (e.g., self-reports from active offenders) and procedures has been exhaustively addressed in previous research, with consistent findings of validity (Jacobs et al., 2003).

Recruitment and data collection

IS research does not have a long tradition of examining crimes, especially from the perspective of active offenders (Mahmood et al., 2010). Therefore, we followed the recruitment protocol recognised and accepted in criminology (Topalli, 2005; Topalli et al., 2020). We interviewed active AFF scammers operating in Cameroon during two field trips and conducted selected follow-up interviews via Voice over Internet Protocol (specifically WhatsApp). Because scammers are wary of exchanging information with strangers, the logistics before and during the interviews were facilitated by three local recruiters over a period of eight years. The first local recruiter was introduced to the first author by an acquaintance who owned a cybercafé in Cameroon[2]. When this recruiter travelled overseas, he introduced the field researcher to another local recruiter. After the second recruiter also travelled overseas, he introduced the researcher to a third and current local recruiter. Unlike the first two recruiters, the third recruiter is a former scammer who was interviewed in 2014 when he was still an active scammer. The third recruiter is currently pursuing a university degree. Critically, the first author of this paper is Cameroonian. His status as a native was necessary to establish initial trust and gain entry into the inner circle of the interviewed scammers. These subjects formed the core group of interviewees for the study and opened access to other scammers via typical networking recruitment techniques (i.e., snowball sampling; see Gundur, 2017; Yingling & McClain, 2015).

Offenders are generally unwilling to spend time with researchers in the absence of at least symbolic compensation for their time and acknowledgement of the value of their information (Topalli et al., 2020). In keeping with common practices in previous research on offenders (Topalli, 2005), we paid the recruiter and offered compensation to the participants. For the first round of interviews, the local acquaintance received CFA 45,000 (roughly USD 77) for his assistance, while the scammers each received CFA 15,000 (roughly USD 26). We conducted the first interviews in 2014 with five scammers. The second round of interviews took place in 2015

[2] The cybercafé owner’s role was limited to introducing the researcher to someone who might have access to scammers.

with 10 scammers. The first and second field trips were to gain an initial understanding of why participants became scammers in the first place and to identify preliminary themes and domains for interviews. Subsequently, we conducted follow-up interviews via VOIP and spoke with two new scammers each in 2018 and 2019, respectively, and one new scammer in 2020. These later interviews were facilitated by a new informant who received CFA 30,000 (roughly 49 USD) for each follow-up interview, while the participants each received CFA 10,000 (roughly 16 USD) per interview. These interviews enabled us to clarify several aspects of our theoretical narrative, including our baseline theory, the role of IT in scamming, how scamming criminality is transmitted in offline and online contexts, and how the process of scamming deception has changed since our previous interviews. Most interviewees were attending middle school, high school, or university at the time they became internet scammers. Three subjects had completed a university degree, and one was attending university at the time of the interviews. The rest were either high school or middle school dropouts. Their online scamming experiences at the time of the interviews ranged from five to 12 years. The offenders brought to us by the recruiters were represented as having made money from AFF scamming—an assertion the scammers confirmed during interviews, which lasted between 45 and 65 minutes.

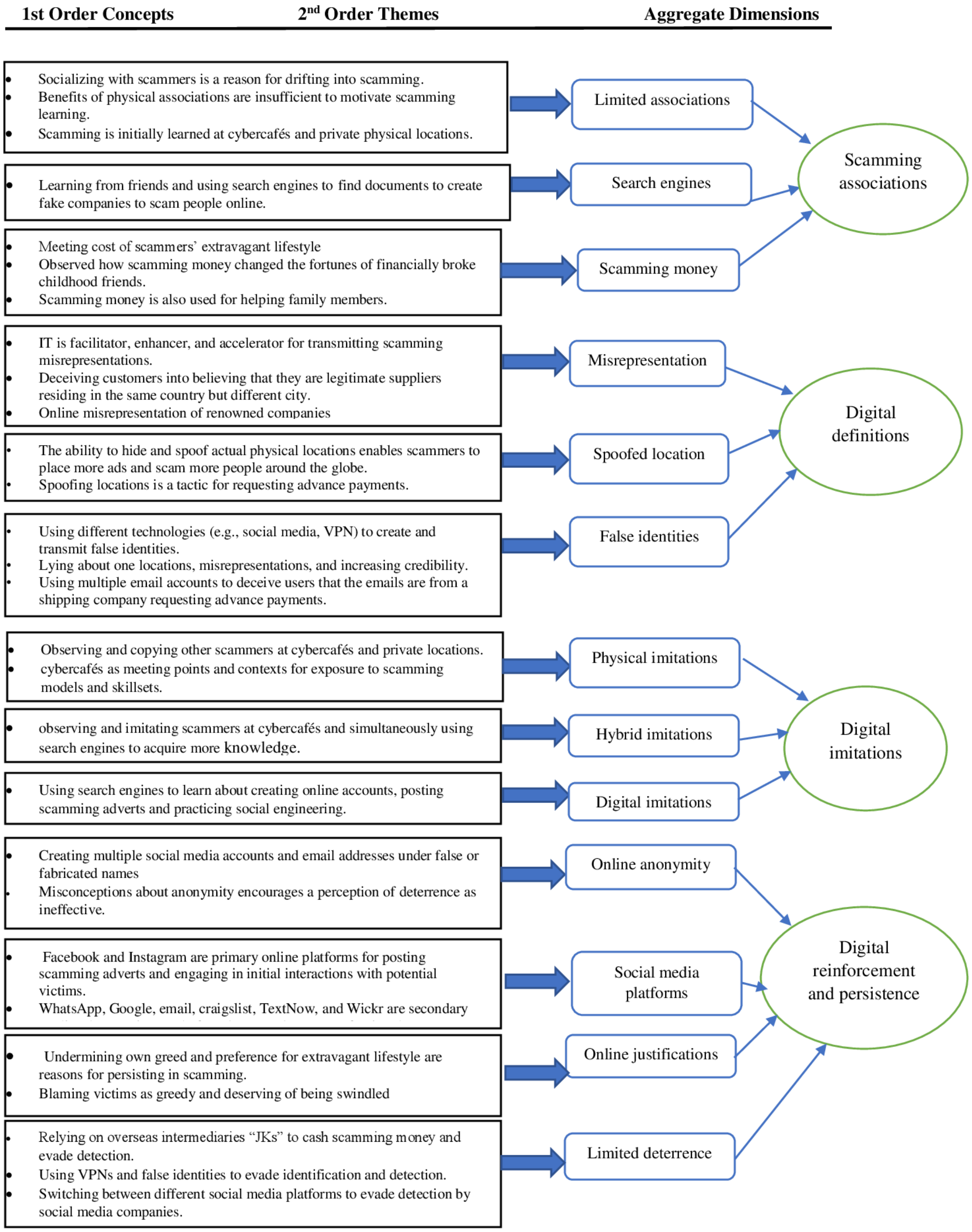
A total of 20 scammers were interviewed for this study. In addition, three scammers were interviewed twice, and four were interviewed three times. Reinterviewing previous subjects is beneficial for numerous reasons. First, as a method of ensuring interview veracity (akin to test-retest reliability; see Golafshani, 2003). Second, using amended protocols based on previous reviews is a method of confirming previous findings or identifying more nuanced categorisations of previously identified concepts and domains (see Castillo-Montoya, 2016). All participants gave permission for their voices to be audio recorded and had the choice of participating in

English or Creole (pidgin English). Typically, the interviews were conducted in English and Creole. Each interview started with questions about the subjects' key activities and experiences before scamming, their age range, and how they became online scammers. At the time of the interviews, four subjects were in their 30s, and the others were in their mid- to late 20s. Subsequently, subjects were asked about the process of acquiring scamming skills (what was learned, how, where, and with whom). Subjects were also asked why they continued scamming and whether they considered quitting. Importantly, we asked them specific questions about the role that IT and other online technologies played in their decisions to pursue AFF scamming. The recruitment of subjects was consistent with human subjects' review protocols at the primary author's institution; we also followed established ethical practices associated with recruiting and interviewing active offenders (see, e.g., Topalli et al., 2020; Wincup, 2017). Furthermore, we adhered to guidelines for establishing concept saturation through repeated interviews and iterative data coding (see Hennink & Kaiser, 2020), a process that allowed us to calibrate the number of respondents we interviewed.

Data analysis

The transcription and coding processes occurred simultaneously (Gioia et al., 2013; Urquhart, 2013). We applied open and selective coding procedures designed to generate theories or models based on interviews or observations (Urquhart, 2013). The analysis involved coding the interviews to identify the meanings of different portions of the data at the sentence and paragraph levels (Urquhart, 2013). The goal was to identify key themes pertaining to why individuals engage in AFF scamming, the extent to which the digital environment facilitated their criminal behaviours, and scammers' reasons for persisting in this form of criminality. Figure 1 shows the final data structure. The analytic process was not linear but recursive and process oriented, continuing until we had a clear grasp of the emerging theoretical relationships.

At the outset, and as noted, the study was inductive and not designed to test a specific theory (Walsham, 2006). However, numerous rounds of preliminary data analysis of scammers' reasoning evoked an SLT explanation of crime. Many inductive approaches recognise such iterations (Eisenhardt, 1989). We then applied SLT as an interpretive lens to understand scammers' motivations for engaging in AFF scams. We later identified selective codes from the final open codes and mapped them to the concepts of association, imitations, definitions, and differential reinforcement from Akers' version of SLT (Akers, 2017; Burgess & Akers, 1966). Because we designed the study to discover cybercontextual (i.e., attributes from the digital environment) influences in AFF scamming, our explanation and proposed model for online scamming accommodate the unique characteristics of the digital context, with specific relevance for AFF scamming. As previously noted, we term this adaptation CTM.



1st Order Concepts	2nd Order Themes	Aggregate Dimensions
- Socializing with scammers is a reason for drifting into scamming. - Benefits of physical associations are insufficient to motivate scamming learning. - Scamming is initially learned at cybercafés and private physical locations.	Limited associations	Scamming engine associations
- Learning from friends and using search engines to find documents to create fake companies to scam people online.	Search engines	
- Meeting cost of scammers' extravagant lifestyle - Observed how scamming money changed the fortunes of financially broke childhood friends. - Scamming money is also used for helping family members.	Scamming money	
- IT is facilitator, enhancer, and accelerator for transmitting scamming misrepresentations. - Deceiving customers into believing that they are legitimate suppliers residing in the same country but different city. - Online misrepresentation of renowned companies	Misrepresentation	Digital definitions
- The ability to hide and spoof actual physical locations enables scammers to place more ads and scam more people around the globe. - Spoofing locations is a tactic for requesting advance payments.	Spoofed location	
- Using different technologies (e.g., social media, VPN) to create and transmit false identities. - Lying about one locations, misrepresentations, and increasing credibility. - Using multiple email accounts to deceive users that the emails are from a shipping company requesting advance payments.	False identities	
- Observing and copying other scammers at cybercafés and private locations. - cybercafés as meeting points and contexts for exposure to scamming models and skillsets.	Physical imitations	Digital imitations
- observing and imitating scammers at cybercafés and simultaneously using search engines to acquire more knowledge.	Hybrid imitations	
- Using search engines to learn about creating online accounts, posting scamming adverts and practicing social engineering.	Digital imitations	
- Creating multiple social media accounts and email addresses under false or fabricated names - Misconceptions about anonymity encourages a perception of deterrence as ineffective.	Online anonymity	Digital reinforcement and persistence
- Facebook and Instagram are primary online platforms for posting scamming adverts and engaging in initial interactions with potential victims. - WhatsApp, Google, email, craigslist, TextNow, and Wickr are secondary	Social media platforms	
- Undermining own greed and preference for extravagant lifestyle are reasons for persisting in scamming. - Blaming victims as greedy and deserving of being swindled	Online justifications	
- Relying on overseas intermediaries "JKs" to cash scamming money and evade detection. - Using VPNs and false identities to evade identification and detection. - Switching between different social media platforms to evade detection by social media companies.	Limited deterrence	

Figure 1. Final data structure.

Findings

How digital platforms facilitate the processes of differential associations

This finding addresses how digital platforms facilitate the processes of differential associations. To recap, differential association in SLT describes how exposure to criminal attitudes, values, norms, and behaviours following socialisation processes with offenders influences a person's attitude and behaviour towards crime, thus providing the social context for the transmission of definitions, imitation, and reinforcement (Akers & Ronald, 2011). To fully grasp why subjects' socialisation experiences with scammers in the physical environment motivated them to take up AFF scamming online, it is important to understand how their association with scammers in the physical environment and the digital context in which the offending takes place influenced their onset decisions. Interviewee 4 said:

> My friends were living a good lifestyle. My friends would ask me: Do you like to wear good clothes and catch beautiful girls? I said yes. Back then, I was not even familiar with the computer. He introduced me to the websites and Facebook. I love the lifestyle. But the lifestyle started with my friends.

This demonstrates the influence of scammer friends but also sheds new light on how digital platforms foment engagement in AFF scamming online. Our analysis revealed that exposure to digital contexts motivates engagement in AFF scamming by giving offenders access to platforms and applications that enhance and accelerate the adoption, imitation, and transmission of criminal knowledge: "I learned quickly. Along the line, it also taught me to do online business" (Interviewee 2). The traditional formulation of SLT predicts that criminal associations that start early, are more frequent, last longer, and are more intensive than noncriminal ones have a stronger effect on behaviour and increase the likelihood that a person will become a criminal. However, our findings demonstrate that these propositions do not hold in the same way in the digital environment. Instead, the combined effects of limited but varied associations with offenders and learning from digital platforms (e.g., search engines and social networking sites) most strongly influenced scamming associations: "I heard about scamming from a cybercafé. I accessed Google and searched for more information. I learned scamming partly on my own. The economy is tough, and the income from scamming helps" (Interviewee 11).

With the prevalence of smartphones, cybercafés are not as prominent in the social learning of scamming. Regardless, interviewees did not require a lifetime of interactions with their scammer friends who taught them AFF scamming techniques. Because of digital affordances, individuals can move from students to scammers-in-the-making and end up becoming full-blown scammers within a matter of hours—a considerably shorter mentoring process than that assumed by traditional SLT. The combination of available scamming models in the physical environment, as well as affordances and more widely available models in the digital environment, eases and shortens the criminal learning process considerably:

> I have been doing scamming since 2006, when I was in Form 5. I had three classmates, and each of them had their motorbikes with people who were working for them. After I discovered that they were doing internet fraud, I asked them to teach me. I didn't put much interest in school again. I learned at a cybercafé. My friends first created me an email account; they taught me about pet scams. Now I do multiple scamming. I sell everything if there is interest and it is on the internet. Now I do it at home on my laptop. (Interviewee 6)

Despite the availability and proximity of scammer models in the physical environment, the digital environment has substantially changed scamming socialisation benefits because online scamming interactions and scamming models are potentially limitless in terms of availability, scale, time, and location. Models are also not restricted to other offenders but include digital artefacts that facilitate the scamming social engineering process, as well as victims who unwittingly volunteer information to scammers for different reasons. The greater internet reach means scammers can target, advertise to, and interact with thousands of people who are otherwise unreachable offline and sell non-existent merchandise on social media and other websites without limitations: “We work throughout the day, and depending on the country, we also work throughout the night. My first experience occurred at night because the victim lived in Australia” (Interviewee 8).

How the digital environment influences AFF scamming definitions and imitation

Again, “definitions” in SLT refer to positive or negative orientations, attitudes, justifications, rationalisations, and excuses that render a given behaviour more right than wrong (positive definition), good than bad (negative definition), or justified than unjustified (neutralising definition; Akers & Jensen, 2006). Although online-based social engineering crimes, such as AFF scamming, maintain many of the characteristics of FtF scamming, there are critical ways in which they function differently. Online AFF scams are executed on digital platforms that provide a variety of behavioural opportunities unavailable in FtF communications. The digital environment affects AFF scamming definitions through various online social engineering techniques employed by scammers to manipulate and deceive unsuspecting buyers. Many of the techniques they practice online would be challenging, even impossible, to pull off successfully in a FtF context. For example, following socialisation with scammers in the physical environment, a large portion of the text-based scamming interactions involve copying and pasting prewritten scam letters, described by interviewees as the “first mail,” the “second mail,” and “airport”:

> I started with pets, pet adoptions, pets for sale. If someone contacts us, we have a first mail, which is fixed. It describes the puppy, for example, its character, etc. The second mail describes the terms of our transaction (e.g., up-front payments). We make the client to understand that we are not in their city; we are in a different city, and the client has to pay for shipping for the merchandise. We ask for their information to enable us to deliver the merchandise. (Interviewee 16)

Subsequently, the scammer sends the first mail in response to a buyer's interest in their scamming advert. The second mail is their reply to a customer's reply to the first mail, and the third mail (also known as the "airport") is to convince the customer that the merchandise will be delivered by an independent logistics company. Typically, the third mail is delivered from a fictitious email account to inform a victim about the delivery schedule and, importantly, about the process for making the first advance payment:

> Once the client sends us that information, we create a shipping agency with Yahoo Mail or Gmail. This other email is for our transportation agency, which is like a pet travel agency, pet transport, or pet delivery. When they send us their contact information, we inform them that we are going to register their pet. After registering the pet, we send an email from our transportation agency as proof that we are processing their package for shipping. (Interviewee 16)

Exposure to criminal definitions which typically begins in the physical environment encourages a person to observe and model not only the beliefs of more experienced offenders but also their behaviours. This is further enhanced because unlike the physical environment, the digital environment exposes scammers to a larger pool of criminal models. This effect is particularly prominent during the initial stages of criminal learning: "As we are online, we see many different things, and I try to do the many different things that I am seeing. We learn online and we learn from people" (Interviewee 17).

Learning, practicing, or imitating social engineering tactics in the service of scamming is more effective and efficient online. The digital environment provides advantages to offenders in terms of targeting, with the ability to approach vastly more potential victims across the globe through a variety of digital platforms (WhatsApp, Facebook, Instagram, etc.) that they employ to communicate with victims, generate multiple identities, spoof locations, maintain anonymity, and stay one step ahead of law enforcement:

> I placed more ads to defraud more customers. If they ask about my location, and I already know that they are in England, I will say that I am in Wales. I emphasise that because of the distance, they must pay for shipment. That's how we start making money. I can ask the buyer for insurance, and that's a lot of money. But it also depends on the product. Insurance money can be as high as US $1700. I can ask for certain other permits, and each time I make sure to give a different schedule for delivery. If the customer is getting smart, I can tell him that the product is dead. (Interviewee 15)

For scamming that takes place in the digital environment, Facebook and Instagram are especially useful for the transmission of definitions of AFF scamming. Scammers' procedural and perceptual skills have led them to become adept at distinguishing between primary online platforms and backup online platforms for engaging in AFF scamming. Primary online platforms (i.e., Facebook and Instagram) are for posting scamming adverts and engaging in initial interactions with potential victims. Facebook and Instagram enable targeted advertising (e.g., through Facebook groups or building Instagram pages about a product), expand the visibility of scamming merchandise, improve the believability of scammers' persuasive communications, and allow live one-on-one chatting. Typically, decisions to switch to a platform are driven by improvements in an offender's crime-specific knowledge and skills in concert with their awareness of technological developments and victims preferred social media platforms:

> Facebook has facilitated business. Chatting with email is much slower. Nowadays, we need to post more ads than before because people are more aware. The Facebook strategy is easier, as we can discuss directly online on a one-on-one basis. As the customers communicate with us, they give us more ideas about defrauding them. (Interviewee 15)

How digital environments affect scammers' online credibility tactics

An important support base for scammers' social engineering tactics and scamming logistics is their strategic use of certain applications as backup online platforms. In such cases, scammers may implement Instagram and Facebook scams in conjunction with these more criminogenic forms of secondary media. Currently, WhatsApp and Google Hangout are the main backup platforms extensively used by scammers, while they occasionally rely on other applications, such as TextNow and Wickr. Their main reason for retaining backup accounts is that Facebook has become much better at detecting and blocking scammer accounts with the help of users. Therefore, to avoid having an account blocked while in the middle of negotiations with a potential victim, scammers shift their communication with a mark to these types of backup accounts. Interviewee 19 stated:

> Facebook officials know that a lot of mafia or crime is occurring through Facebook, so now they are monitoring accounts a lot. If they suspect that an account is engaging in suspicious behaviour, they instantly delete that account…We even use online Google number in case they block our Facebook accounts and still communicate in the form of text messages. There are also different apps that we download to communicate. Currently, we are using Google Voice's Hangout, WhatsApp, or TextNow app. We use them as a secondary means of communicating with a client, especially when we are at a level where you begin to suspect that Facebook may block our account. We take the clients' number and transfer the communication to TextNow or Google Hangout.

Many of the different social engineering techniques scammers employ serve to increase their credibility or trustworthiness. Once scammers successfully allay victims' concerns (for instance, “We scam them through their trust,” Interviewee 15 stated), they demonstrate expertise by asking victims “expert questions,” which highlight scammers’ knowledge of the offered merchandise. For example, in scams where pets are offered for adoption “for free,” scammers send interested customers a list of questions that targets the most promising victims: They choose “pet lovers” with a history of owning specific kinds of animals (easy enough to discern from the victims’ public Facebook pages) while at the same time engaging in a fair amount of research on the animals in question so as to showcase their knowledge and develop a bond with the target: “Knowhow is important. The customer can ask questions such as has the pet received veterinary checks? Is it up to date on its vaccines? They also ask that you present the documents” (Interviewee 7).

Expertise also pertains to the ability to search for fake documentation online, edit it, and transmit it to victims as proof or evidence of the legitimacy of a proposed transaction, as illustrated here: “So, we go to Google and copy the documents, edit them, and send them. There are some people who can’t go to Google and remove such documents and do editing” (Interviewee 4).

Furthermore, the digital environment allows scammers and scammers-in-the-making to assume multiple roles (i.e., roleplaying) while selling non-existent digital merchandise, spoof and lie about their physical locations, freely create multiple digital profiles, migrate from one platform to another at low cost, and hide (anonymise) behind text messages in live or asynchronous communications. Interviewee 1 stated:

> As customers write, I see it as an opportunity. I go to them with a different email address. I reduce the price to make the customer happy because he begins to think that I am genuine. I treat my customer nicely. He doesn’t want a high price. If I don’t reduce the price, another scammer will scam him at a lower price.

In addition to the social engineering techniques described above, scammers' orchestration of credibility to increase the persuasiveness of their deceptive tactics (e.g., through roleplaying, fake profiles, and spoofed locations) and thus entice individuals into making advance payments is further illustrated in Table 3. This process is facilitated by the digital-level factors associated with learning cybercrime strategies from others. Unlike traditional scammers in the physical environment, online scammers have the added advantage of quicker learning facilitated by search engines, digital documents that can be copied from one environment and pasted on another, and theoretically limitless interactions with victims and other offenders. Therefore, the identified attributes in Table 3 explain why scammers' social engineering practices are so successful online.

Table 3. Additional social engineering techniques displayed by AFF scammers.

Role playing	"I started doing dating scams where I disguise as a woman to make the victim fall in love with me. For us to meet, they need to send me money to pay my flight." (Interviewee 2)
Geospatial locations	"When the customer says he is in Texas, I say I am in Montana. He will never come to take it, because the distance is long. I try to eat through the delivery, so the customer will request that I should deliver." (Interviewee 6). "We make the client to understand that we are not in their city. We are in a different city, and the client has to pay for shipping for the merchandise." (Interviewee 16)
Digital profiles	"We create a normal Facebook account and use the profile picture of any white person." (Interviewee 19). "From their profile pages, we determine those people who like marijuana, send them friend requests, and if they accept your request, they will likely check out my profile page and realise that I am a supplier." (Interviewee 20). "We create an account, but we need to build the account in the form of the type of product we want to supply. If it's marijuana, we build it in the form of marijuana; if it's pills or pets, we build our profiles to advertise those products." (Interviewee 16). "Yes, we were changing email accounts often. They are not real email accounts. I could just guess an email account in my head and create a new one." (Interviewee 19).
Low migration costs	"After doing pet scamming, I realised that advertising products in bulk makes sense so I moved to fertilisers, I posted sites for fertilisers, i.e., different types of fertilisers and I got a customer." (Interviewee 3)
Physical and text-based online interactions	"I first saw the computer as a means for learning. I was a student, learning maintenance and networking, and my initial transactions involved improving my knowledge. Then my friends became scammers, and they suggested it to me." (Interviewee 13) "He taught me about computers, how to place ads, if I have a contact, how I should reply, and, he taught me how to react, what to say." (Interviewee 10)

Digital merchandise and digital environment	“I put an add about a merchandise I didn’t have. Customers started contacting me to see the products. To convince them, it depends on how they first wrote to me.” (Interviewee 12). “I told her that when you make the payment, send me a scanned copy of the details. After she paid, I told her that we shall proceed with the transportation in an hour’s time.” (Interviewee 5). “On Facebook, we create a Facebook page and post pictures of different types of marijuana. We search the marijuana community through Facebook search bar and apply to become members. From their profile pages, we determine those people who like marijuana, send them friend requests, and if they accept my request, they will likely check out my profile page and realise that I am a supplier. If they are interested, they contact me, and I will give them my Google Voice or Wickr app address, then we can begin to discuss better.” (Interviewee 20)
Imitation	“I imitated what others had done and edited it to suit my own product.” (Interviewee 3) “At the cybercafé, I saw those who were doing scamming, and they most often had money. I began asking and talking to them. Then, I decided to become a scammer, too. I also wanted money, so I began copying what they were doing. They discussed with Westerners, and the Westerners would send them money.” (Interviewee 14)

How the digital environment enhances the concept of reinforcements

Recall that differential reinforcement refers to positive and negative outcomes or reactions anticipated to result from an emulated act. SLT posits that past, present, and future anticipated rewards and punishments influence a person’s decision to participate and persist in crime (Akers & Jennings, 2009). This premise explains how scammers are reinforced to engage in scamming and how they persist in the face of challenges largely in response to the advantages and affordances of the digital environment. Such criminogenic attributes from online contexts reinforce scammers to continue scamming and encourage them to persist in their offending. These include previous scamming rewards, deterrence perceptions, punishment avoidance, online anonymity, and online justifications.

Our findings show that scamming continues to thrive because offenders exploit technological affordances that are particularly effective at transcending physical world–based limitations on learning processes. A host of built-in characteristics of social media platforms makes it easy for scammers to create and delete accounts, use false identities, acquire and use phone numbers (for verification), and spoof or lie about their physical locations. IT further provides benefits to scammers in targeting and taking advantage of victims through various commercial online platforms (WhatsApp, Facebook, Instagram, etc.). Such online-based facilitative systems accelerate and strengthen the learning processes previously limited by traditional physical world contextual learning. Interviewee 17 stated:

> We get the American IP through a Google search. We just go to free U.S. IP proxies; there we can get fresh American IP, which are constantly changing per second. They are creating new IPs every second. My IP is from the state of Oregon, and my number, too, is from that state. We use an American IP to change the proxy of my phone, and our phone's setting changes automatically.

Subsequently, when a given mode of communication or commerce is no longer safe or advantageous for scammers to use, the costs of switching to new online services are minimal: "He contacted me after seeing my pictures on Instagram, I took his number and called him on my Google Voice. Then, I gave directions on how he should make payments" (Interviewee 18). This makes cyber-contextualised learning processes more fluid and less subject to otherwise discouraging bouts of failure that would interfere with learning, as traditionally conceptualised in SLT.

Furthermore, because scamming operations do not take place FtF, the salience and immediacy of the impact of scammers' actions on themselves and others are somewhat dulled. This dissociative and anonymising influence of online environments produces an overall disinhibition effect on scammers that facilitates their use of excuses, justifications, and neutralisations to counter their guilt and fear of consequences for their transgressions. We found that scammers often provided such justifications to assuage the guilt of swindling particularly vulnerable individuals (e.g., a single mother or the elderly) to support their own lifestyle of conspicuous spending. They are also a means for scammers to undermine the perception that they are "greedy" by blaming their actions on an absence of legitimate opportunities while portraying their victims as the ones who are avaricious. However, offenders' need for money is mainly a product of their extravagant lifestyles:

> The day I got the money transfer, I was happy. Internationally, the merchandise doesn't sell like that. They know the price. The money they want to pay is not even half the price of the cost of the goods they want, or they are willing to pay. They come to us because they think we are desperate. There is no reason to even supply half, so don't even supply anything. The international price is on the internet, and now they want for less than half that price. I am totally the victim. They prefer the lower prices, but it comes at a cost. The buyer doesn't want a high price. If I don't reduce the price, someone else will scam him at a lower price. (Interviewee 1)

How AFF scammers persist in their criminality

The concept of reinforcement, largely based on the experiences of past rewards (e.g., scamming money), and the affordances of the digital environment encourage scammers to persist in their criminality. The digital environment attributes weaken anti-scamming deterrence measures, providing scammers with a variety of alternative platforms when a given online medium becomes problematic or hostile to their criminal activities. In previous passages, we described how scammers leverage primary and secondary platforms to facilitate the uninterrupted perpetration of their scams. The attributes of these platforms also encourage persistence in scamming:

> We also do scams on Instagram. I use Facebook and Instagram, and WhatsApp. What I do is when a person shows interest on Instagram, I take their contact number and move

> the communication to WhatsApp because we have American numbers here in Cameroon. We buy the numbers by using American credit cards. (Interviewee 17)

The inherent flexibility and interchangeability of platforms facilitate their persistence. Thus, AFF scammers perceive the digital environment differently from traditional offenders, mainly because the fluidity of the online context facilitates their motivations and foments the acquisition of specialised offending knowledge. Furthermore, the absence of active deterrence and opportunities in digital and physical environments that enable scammers to avoid punishment also encourage scamming persistence. Generally, when offenders learn how to avoid the negative or unpleasant consequences of a behaviour, they are more likely to repeat that behaviour (Akers & Jennings, 2009). The digital environment enhances negative reinforcement or punishment avoidance through online anonymity, and scammers' perceptions of anonymity lead them to downplay the risk of apprehension and exaggerate the rewards of scamming:

> I was aware of the risks of scamming; that is why I don't use cybercafés. I have my own internet key at home so that they can't track me. It is difficult to track me because Cameroon is less developed, so it is not too fast to track me online. I don't use my real name. I steal others' identity online. (Interviewee 9)

However, scammers are not always successful. The subjects conceded that defrauding people online had recently become somewhat more challenging because of increased user awareness. In some cases, this awareness has been facilitated through government communication efforts. That said, the rewards from scamming reinforce them to persist in criminality. The benefits continue to outweigh the risks because attributes of the digital environment that enhance scamming activities often simultaneously make effective deterrence more difficult to achieve: "Most of our targets receive tips from their governments against financial fraud, so it is increasingly hard to catch a JK [victim]. Most of them are fully aware, so it is tough to scam someone" (Interviewee 4).

Many of the strategies scammers employ (e.g., falsifying their identities and locations, and using temporary fraudulent email and Facebook accounts) are based on affordances of digital environments. This serves to foster scammers' belief that it is impossible for their activities to be traced back to them. For instance, when asked whether they feared being tracked through their registered smartphones, Interviewee 12 responded, "Even if they track it, I am not worried. I don't think they will find the time to leave the West to come to Africa to find me." Thus, AFF scammers have criminogenic beliefs about digital technologies that facilitate their operations in many ways. Although improvements in technology (related to deterrence and detection) should make offenders more concerned about the prospect of apprehension, they remain undeterred because digital contexts do not provide enough salient and visible prevention. Although technological advancements should make it easier for authorities to track and impede the activities of scammers, they continue to believe that the same ineffective deterrence measures they have grown accustomed to will hold:

> No, I don't fear being caught. At first, we can say we were afraid of the police. But now we plan all the scams from our homes, and when the client makes the payment, it is sent to our overseas pickup. The pickup sends the money to us, even if it is through mobile money, so there is nothing to fear. The police will hardly see me with receipts that I am from a bank and have received money from strange contacts or names. We have already outsmarted law enforcement. Law enforcement cannot be a problem. (Interviewee 18)

Furthermore, our findings demonstrate how scammers are already changing their tactics in response to shifts in deterrence measures deployed by social media networks. Scammers acquire new backup accounts or switch to current backup accounts as replacements for primary accounts; scammers also abandon existing primary and backup accounts entirely for emerging popular platforms. Interviewees maintained that the increased proliferation and use of smartphones served only to facilitate scamming by further loosening locational boundaries:

> Everything is much easier. We use our smartphones. Even laptops are not very useful again. We sometimes use computers when we want to post our ads. But now we mostly work drug scams, so we only use our phones. We don't need computers; anywhere we sit we can work from our phones whether at a bar, anywhere…We have everything on our phones. Whether you want a video or pictures, we send through our phones. (Interviewee 16)

Importantly, deterrence perceptions may also be affected by the locale from which scammers currently operate. African scammers recognise that even when counterdiction efforts by law enforcement are more likely, they can find ways to avoid them. For example, subjects mentioned bribing law enforcement or colluding with bank officials. Although such actions may be less likely in countries with more robust legal systems and less corruption, the perceptions and opportunistic behaviours of these scammers encourage and reinforce their criminality:

> The government policy to deter us is very ineffective. When the police come, they are asking for their own share of the scamming money. They catch us through the money. Also, when the police come, it means a scammer has informed them. Some scammers collude with the police and they then share the money with the police officers. (Interviewee 2)

Discussion

Although AFF scamming predates the internet, it has become a major cybersecurity problem because of the internet. Our findings have demonstrated how scammers engage in both the FtF and digital environments to swindle their victims. Specifically, this study was designed to address two research problems. First, how the digital environment motivates individuals to engage and persist in AFF scamming. Second, and driven by our empirical analysis of data from active scammers, how social learning theories of criminal behaviour are appropriate and inappropriate for understanding and predicting offending behaviour online. We organised the interpretations of our findings according to our research questions.

RQ1: How does the digital environment motivate individuals to engage and persist in AFF scamming?

We address this question by focusing on the digitalisation of AFF scamming, the nature of criminal associations, and imitational learning in the digital environment, and why the digital environment motivates reinforcement and persistence behaviours.

Digitalisation of AFF scamming, scamming associations, and imitational learning. We identified limited associations and search engines as two components that directly influence scamming associations for AFF scamming offences that take place online. First, the *limited associations* attribute (for victims and offenders alike) suggests that for digital offences such as AFF scamming, socialisation with scammers starts in the physical environment. However, the subsequent shift to the digital environment accelerates learning and crime involvement as offenders use search engines to find and retrieve additional documents and information to facilitate the scamming deception interaction process. Second, the *search engine* attribute highlights how scammers and scammers-in-the-making depend on this artefact to seek out and access information, as well as download documents relevant for learning how to persuade targeted individuals during a social engineering process.

Furthermore, our finding illustrates how the digital environment influences scamming definitions and imitations through scammers' social engineering techniques. It enables scammers to make deceptive scamming messages credible online, which entices online users to advance payments to scammers. Like scamming associations, the *online imitation* attribute stresses that scammers filter and adapt their observations in response to a wide pool of online models, ranging from other offenders and victims to social media platforms. The digital environment enables scammers to project themselves on social media platforms and in email communications as legitimate suppliers of merchandise through *misrepresentations,* which comprise three digitally enabled social engineering definitions: *false suppliers, false identities,* and *spoofed locations*. Scammers' techniques demonstrate how online offenders use digital platforms to create multiple fake profiles while simultaneously building trust and credibility, playing multiple roles, and spoofing their locations. These social engineering techniques increase victims' perceptions of scammers' legitimacy and believability with the goal of receiving advance payments.

AFF scamming digital reinforcement and persistence. The first part of this finding explains how the digital environment influences scamming reinforcements through a digital reinforcement concept and several cybercontextual attributes that influence it. *Digital reinforcement* attributes include social media platform affordances, online anonymity, weak deterrence perception, and online justification. They are reinforced by previous successful scamming experiences as well as scammers' concomitant expectations of future rewards. First, the attributes of *social media platforms* enhance and accelerate scamming activity by making it easy for scammers to create and delete accounts, use false identities, and apply false locations to deceive users. Second, the *online anonymity* attribute emphasises how the digital environment encourages scammers' behaviours by enhancing negative reinforcement or punishment avoidance. Anonymity serves to increase scammers' confidence that they can operate with impunity and makes the prospect of disapproval, punishment, or retaliation less salient. Third, and relatedly, the *limited deterrence* perception attribute explains why scammers are not concerned about being caught. Because online anonymity makes effective deterrence more difficult to achieve, it reinforces offenders' perceptions that they can continue realising rewards from their present and future scamming behaviours with impunity. Fourth, we identified an *online justification* attribute caused by the distant and mostly text-based nature of scamming interactions with victims. This attribute explains why scammers very easily rationalise their actions and why their justifications are less morally demanding to invoke online than FtF interactions.

The second part of the finding describes and explains how the digital environment enables scammers' persistence in their criminality. Based on our previous findings, we identified a *digital persistent* attribute that is facilitated by primary and backup online platforms, search engines, ease of platform migration and adaptation, and limited deterrence perception. In essence, digital persistence explains why fraudsters show resilience despite the challenges of scamming people online. The primary online platforms that scammers use in conjunction with other backup platforms (e.g., WhatsApp) enable them to deceive online buyers effectively and efficiently in terms of time (e.g., real-time communications) and financial costs (e.g., low migration costs), but without punishment. Our findings suggest that scammers tend to always find ways to evolve their tactics in line with technological advancements and deterrence measures, such as using backup accounts or switching to primary accounts to evade deterrence measures and increase their likelihood of scamming success. In addition, online anonymity and social media attributes weaken punishments and make deterrence harder to enforce. Over time, this acts as a reinforcement for persistent scamming.

RQ2: How are social learning theories of behaviour appropriate and inappropriate for understanding and predicting offending behaviour online?

Following our second research question, we observed that little empirical research has focused on the offenders themselves, and few studies have also empirically explained the reach of the digital environment in explaining online scammers' motivations. Although SLT is useful for identifying a process in which offenders learn to become scammers in the physical environment, the theory does not offer much details for explaining the online context of AFF scamming. Accordingly, we propose a cybercontextual transmission model (Figure 2) to explain how the digital environment accounts for offenders' online scamming behaviours. The model also demonstrates how we reformulate Akers' SLT by accounting for cyber-contextualised social learning attributes that foster the uniqueness of the digital environment. The elements of the model are described in Table 4.

CTM contends that the traditional environmental attributes espoused in Akers' formulation of SLT remain relevant for understanding how individuals are initially exposed to online offences, such as AFF scamming. However, CTM also posits that these attributes largely change once the learning process enters the digital environment. The cyber-context or digital environment provides new forms of knowledge and belief transmission for associating, communicating, and sharing ideas (e.g., email and WhatsApp). It gives offenders access to an unlimited pool of imitation models (including victims who unwittingly share tips with offenders). Definitions in the digital context are influenced by scammers' social engineering techniques, and reinforcements and persistence in the digital context are affected by digital environmental attributes, online anonymity, justifications for scamming, and scammers' perceptions of online deterrence.

Therefore, CTM highlights how digital technologies offer scammers possibilities for creating and owning many online accounts and profiles, as they simultaneously play multiple roles while using several online platforms to engage in AFF scams. CTM also explains that the digital context of scamming deception enables scammers to hide behind text messages in live or asynchronous communications, choose locations that suit the context of the deception process, and evolve their online practices in ways that maximise the benefits of online anonymity and make effective deterrence more difficult to achieve.

Building on Akers' SLT, CTM proposes that the four major concepts in SLT—scamming associations, digital definitions, digital imitations, and digital reinforcements and persistence—are mainly influenced by attributes from the digital environment and scammers' social engineering practices. In essence, CTM is based on empirically derived cyber concepts that conceptually build on Akers' traditional formulation of criminal learning but differ functionally from it. Consequently, CTM explains how the digital environment affects AFF scammers' motivations and scamming practices.

Figure 2 presents our cyber-contextualisation model for AFF scamming. We used different colours to distinguish the social learning core attributes of AFF scamming (scamming associations, digital definitions, digital imitations, and digital reinforcement and persistence) and their respective cybercontextual attributes that influence AFF scamming. The core attributes make up proposed conceptual model (i.e., CTM).

To summarize, the CTM conceptual model in Fig. 2 comprises the same core concepts from Akers' SLT (i.e., differential associations, definitions, imitations, and reinforcements). However, in the online environment, these concepts function differently.

Table 4 explains how the new concepts from our study extend and differ from SLT (Akers, 2017). For instance, scamming associations comprises limited associations and search engines that challenge the existing explanation in SLT about functioning of online criminal learning. We also identify misrepresentations as a digital definition and online anonymity, social media platforms, online justifications, and limited deterrence as forms of online digital reinforcement. These new attributes suggest that while Akers SLT remains relevant because the core learning processes are the same, they manifest differently in the online context.

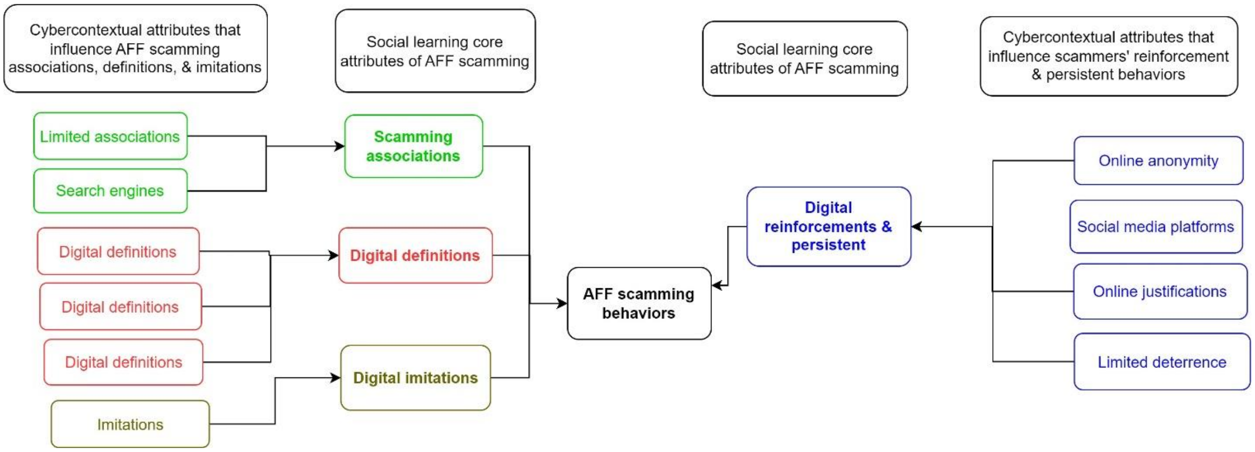

Cybercontextual attributes that influence AFF scamming associations, definitions, & imitations
Social learning core attributes of AFF scamming
Social learning core attributes of AFF scamming
Cybercontextual attributes that influence scammers' reinforcement & persistent behaviors
Limited associations
Search engines
Scamming associations
Digital definitions
Digital definitions
Digital definitions
Digital definitions
Imitations
Digital imitations
AFF scamming behaviors
Digital reinforcements & persistent
Online anonymity
Social media platforms
Online justifications
Limited deterrence

Figure 2. Cybercontextual transmission model for AFF scamming.

Table 4. Explanation of concepts.

Scamming associations: Limited associations Search engines	***Scamming associations*** refer to the difference means by which scammers acquire and transmit new or existing forms of knowledge. Specifically, this happens through limited associations (with successful scammers) and reliance on search engines) ***Limited associations*** are the combined effects of limited but varied associations with offenders and learning from digital platforms (e.g., search engines and social networking sites) and victims: *My friends first created me an email account. They taught me about pet scams. Now I do multiple scamming. I sell everything if there is interest, and it is on the internet*. (Interviewee 6) ***Search engines*** are online platforms that facilitate criminal learning and document falsification by enabling scammers to seek out, access, and download information relevant for deceiving individuals: *I heard about scamming from a cybercafé. I accessed Google and searched for more information. I learned scamming partly on my own*. (Interviewee 11)
Digital definitions: Misrepresentations (false suppliers, false identities, and location spoofing)	***Definitions*** in the digital context are influenced by scammers' social engineering techniques ***Misrepresentation*** is a false statement about a material fact that scammers make to deceive individuals into perceiving them as legitimate suppliers of merchandise. It serves to mislead individuals into perceiving scammers as legitimate suppliers of merchandise. We find that misrepresentation comprises three main elements: false suppliers of goods and services, false identities, and location spoofing. While some scammers misrepresent themselves without creating and changing their identities, others misrepresent themselves through false or stolen identities.

	False suppliers: AFF scammers deceive people about the true nature of a transaction or service through false statements or material omissions about a fact. For example, intentionally misleading people about the location, quality, existence of merchandise, or their reputation. ***False identities*** are deployed through multiple fake social media accounts that allow scammers to misrepresent themselves by claiming whatever identity may suit their deception scheme while simultaneously hiding from law enforcement *As customers write, I see it as an opportunity. I go to them with a different email address. I reduce the price to make the customer happy because he begins to think that I am genuine.* (Interviewee 1) ***Location spoofing*** is a tactic employed to mislead users about their physical locations and create an opportunity for incidental transportation, which is a form of advance fee payment that is required before merchandise can be shipped. *I placed more ads to defraud more customers. If they ask about my location, and I already know that they are in England, I will say that I am in Wales. I emphasise that because of the distance, they must pay for shipment. That's how we start making money.* (Interviewee 15)
Imitations: Digital imitations	***Imitations*** Involves observing and modelling behaviours that increase criminality. But imitation only plays an important role in initiating deviant behaviour. ***Digital imitation****:* Involves socializing, observing, and modelling behaviours that increase the likelihood of scamming success in the physical and online environments. Crucially, digital imitation is sustained through differential association with scammers because success often depends on loose collaborations and sharing of new ideas. *I imitated what others had done and edited it to suit my own product*. (Interviewee 3) *At the cybercafé, I saw those who were doing scamming, and they most often had money. I began asking and talking to them. I also wanted money, so I began copying what they were doing* (Interviewee 14)
Digital reinforcement and persistence: Online anonymity Social media platforms Online justifications Limited deterrence	***Reinforcements and persistence*** in the digital context are affected by digital environmental attributes, online anonymity, and justifications for scamming. ***Online anonymity***: The degree to which scammers believe that their personal identities and locations will remain hidden, and they cannot be held accountable for their scamming criminality. *I placed more ads to defraud more customers. If they ask about my location, and I already know that they are in England, I will say that I am in Wales.* (Interviewee 15) *I was aware of the risks of scamming; that is why I don't use cybercafés. I have my own internet key at home so that they can't track me. It is difficult to track me because Cameroon is less developed, so it is not too fast to track me online.* (Interviewee 9) ***Social media platforms***: Online venues where scammers post adverts, engage victims in multiple interactions, and manipulate them into making advance payments. Social media platforms can be primary (e.g., Facebook and Instagram) or backup (e.g., WhatsApp). *Facebook officials know that a lot of mafia or crime is occurring through Facebook, so now they are monitoring accounts a lot. If they suspect that an account is engaging in suspicious behaviour, they instantly delete that account…We even use online Google number in case they block our Facebook accounts and still communicate in the form of text messages. There are also different apps that we download to communicate. Currently, we are using Google Voice's Hangout, WhatsApp, or TextNow app. We use them as a secondary means*

	of communicating with a client, especially when we are at a level where you begin to suspect that Facebook may block our account (Interviewee 19) **Online justifications**: Excuses from scammers' experiences in physical and online environments that they invoke to rationalise or justify their criminality and thus persist in it. *Internationally, the merchandise doesn't sell like that. They know the price. The money they want to pay is not even half the price of the cost of the goods they want, or they are willing to pay. They come to us because they think we are desperate. There is no reason to even supply half, so don't even supply anything. The international price is on the internet and now they want for less than half that price. I am totally the victim.* (Interviewee 1)

Contributions

This study contributes to the behavioural IS security literature and explains how cybercontextual attributes motivate and facilitate individuals to perpetrate online social engineering attacks. Our first contribution identifies digital attributes that explain the ways in which the digital environment motivates and influences individuals to engage and persist in online scamming offences. Previous research investigating the role of digital factors in social engineering attacks and cyber-offences has established that the online environment instigates cyber-offences through its effects on human cognition and behaviour. However, despite the prevalence of such scamming offences and several calls in leading IS journals for studies on "black hat" cybercriminals, little research has addressed this problem. We address such calls using data from active AFF scammers and propose a social learning explanation that emphasises the role of digital attributes in scamming motivation (i.e., scamming associations, digital definitions, digital imitations, and digital reinforcement and persistence; see Figure 1). In highlighting and clarifying the role of the digital environment in online scamming offences, our contributions also demonstrate that the financial motive explanation in the literature is a relevant but insufficient account. First, scamming associations suggest that learning through socialisations is not limited to other offenders—or offenders who are in close physical proximity—but extends to a theoretically unlimited pool of online models ranging from interactions with victims and search engines. Second, scamming definitions and imitations demonstrate how AFF scammers employ social engineering techniques to project themselves as credible and legitimate on social media platforms and in email communications to entice individuals into making advance payments to them. The ability to do this is acquired through digitally facilitated social learning processes. As shown in Figure 1, we identified three forms of misrepresentations largely influenced by digital technology that influence Akers' traditional idea of criminal definitions: false suppliers of goods and services, creation of false identities, and location spoofing. Third, we identified several digital reinforcements (social media platform attributes, online anonymity, and online disinhibition) that strengthen scammers' expectations of future rewards and motivate their resolve to persist in scamming criminality. In addition, we identified a digital persistent attribute comprising primary and backup online platforms, search engines, ease of platform migration and adaptation, and weak deterrence that encourages scamming persistence.

Our first contribution identifies and explains the cybercontextual social learning attributes that influence engagement and persistence in AFF scamming. Our second contribution underscores how traditional criminological theories, such as SLT of crime, cannot sufficiently account for cyber-offences such as AFF scamming.

Accordingly, we propose CTM as a conceptual framework for AFF scamming and other offences that considers the unique characteristics of the digital medium. CTM is designed to account for the unique ways in which digital environments mediate the perpetration of offences and responses to them in ways that traditional criminological theories rooted in physical world assumptions cannot. The theory, which derives core principles from SLT, is similarly inappropriate for describing and predicting how the beliefs, techniques, and tactics of scamming are transmitted in FtF crime.

This finding demonstrates the limited applicability of Akers' SLT for explaining online offences, such as AFF scamming. CTM suggests that exposure to cybercontextual attributes motivates engagement in AFF scamming by giving offenders access to platforms and applications that enhance and accelerate the adoption, imitation, and transmission of criminal knowledge beyond what is possible or normative via FtF interactions. Thus, this contribution demonstrates some key weaknesses in the adequacy of traditional learning theories of crime for accounting for online offences.

The identified limitations in SLT led us to propose CTM as an IT-specific conceptual framework for deceptive online practices. CTM draws from the underlying core concepts in SLT because they rely on core principles of social cognition that are relevant in describing aspects of online crime, such as online scamming. However, unlike SLT, the components of CTM are influenced by exposure to the cyber or digital environment (see Figure 1). Through our identified cybercontextual social learning attributes, CTM describes how scamming associations, models, and the digital environment induce individuals to accept and incorporate definitions favourable to cybercrime, with more intense and widespread consequences. Accordingly, our cybercontextual attributes revise Akers' SLT, highlight the limitations of traditional SLT in explaining online offending, and contribute a rich conceptualisation to behavioural security research and SLT.

Implications for research, practice, and limitations

The first research implication of this study is that it clarifies the limits of traditional theories of crime, such as SLT, to explain and predict online offences, such as AFF scamming. Specifically, our findings first show that SLT's propositions are insufficient to accurately describe or predict offending (such as AFF scamming) in the digital environment. Essentially, this reifies the stance by IS scholars that the field should develop and adopt new theories that integrate the IT attributes and contexts of specific cybercrimes (Hong et al. 2013). The cyber-contextualisation conceptual framework (Figure 2) can serve as an important starting platform for testing and formulating our identified cybercontextual attributes. AFF scamming is just one example. Hacking, cyber grooming of children, and cyberterrorism are some new forms of crime that traditional criminology approaches may be ill-equipped to address, primarily because of that discipline's emphasis on physical world–based notions of crime causation, human interaction, and human behaviour. Therefore, developing new theories that integrate IT attributes and contexts is critical to studying and understanding offending from an IS perspective.

The second implication is that our explanation of social engineering techniques from the offenders' perspective adds to the burgeoning IS research on the topic, which has largely been conducted from the victims' viewpoint. Specifically, we recommend a shift in emphasis from explaining the behaviour of offenders through data collected from surrogates (friends and relatives of offenders) and reviews of newspapers to longitudinal (ethnographic) studies that extract data from the offenders themselves, as well as law enforcement officials directly involved in combatting AFF scamming. Because online offending is intimately tied to current trends in social media, active offender research and real-time data collection from law enforcement are particularly critical for establishing up-to-date, relevant information about current and emerging trends in cybercrime. Such an orientation towards research would directly address several issues raised by this study. Consistent with previous research (Jamieson et al., 2012), our perspective is that AFF scamming techniques are likely to change or evolve over time. Importantly, because our research is among the first to consider scammers' tactics from the offenders' perspective, this knowledge provides a starting point to document and understand how offenders' social engineering techniques emerge and evolve over time.

For practice, we observe from the data that scammers are mostly interested in convincing, persuading, and deceiving only a few users into making advance payments. The scammers recognise that most users have become aware of their tactics. However, the prevailing anti-scamming recommendations remain focused on victims of social engineering attacks. Although empowering users to protect themselves against social engineering attacks is laudable, and the scammers we interviewed acknowledged its effectiveness, improvements in technology and scammers' persuasive skills continue to enhance scammers' credibility. Therefore, we recommend that researchers, practitioners, and law enforcement focus on changing the behaviours of motivated scammers, especially because they employ neutralising definitions or justifications to avoid experiencing guilt regarding their offending (Sykes & Matza, 1957; Siponen & Vance, 2010). Neutralisation theory suggests that such individuals may provide the most effective target audience to dissuade from offending. Furthermore, as the friendship activities that motivate individuals to begin committing online scamming occur mainly in schools, students should be educated about the risks of becoming scammers because of socialising with scammers. However, there are challenges for programmes targeting scammers' activities. The ease of learning the techniques of committing scamming and the fact that these techniques are dynamic, changing as users' knowledge and technology change, indicate a race between scammers and the protective measures against their activity. That some victims who have been warned by their banks or relatives choose to listen to scammers is problematic for campaigns to protect against scamming. We recommend reducing these hurdles through sanctions against scammers that are certain and visible.

Despite the benefits of relying on interviews from active (non-institutionalised) scammers, this approach has limitations, including difficulty recruiting offenders, trusting that they follow interview protocol expectations, and relying on the truthfulness of their accounts (Topalli et al., 2020). Active offenders are also reluctant to interact with outsiders and discuss their past criminal histories for fear of implicating themselves (Jacobs, 1999; Topalli, 2005). Although the limitation of our approach can be overcome by employing a participant-observation method, this approach is neither ethically feasible nor safe. Interviewing active (non-institutionalised) offenders provides unique insights into the foreground of offending, because such offenders (unlike their incarcerated counterparts) have fresh memories of their crimes (Topalli et al., 2020). Nevertheless, we recommend follow-up studies to examine the concepts delineated in this paper from the perspectives of law enforcement, corporate and government regulators, and victims. However, we emphasise that offenders provide a unique perspective. Only they understand and can discuss their motivations for engaging in scamming directly, as well as when, where, and how they make decisions about when to desist or persist in such efforts. Law enforcement may have important information related to AFF offending as an activity, but their own beliefs about the motivation of offenders are unlikely to be as valuable as hearing it from the offenders themselves.

Furthermore, a key limitation of CTM is that, because it is derived from the core principles of SLT, it is similarly inappropriate for describing and predicting how beliefs, techniques, and tactics of scamming are transmitted in FtF crime. Although we discussed the role of friends and socialisation benefits in the physical environment, this model does not consider the wider social and cultural issues in the local environment that contribute to people’s reasons for becoming scammers. While the social learning process was dominant in the collected data, we observed that attributes from the local environment were also evident, such as stressors from the physical environment. Our analysis revealed that scammers employ neutralisations and justifications to cope with their criminality and persist in it. However, there are other plausible perspectives that could be helpful in addressing the etiology and perpetration of AFF scamming other than one that is SLT-based. Therefore, we recommend that future research examine AFF scamming from the perspectives of strain theory (Agnew, 1992), social control theories (Gottfredson & Hirschi, 1990; Freilich &Newmann, 2015), and rational choice theories (Cornish & Clarke, 2016) of crime.

Conclusion

This study was designed to understand how the digital environment facilitates and motivates engagement and persistence in AFF scamming, as well as affirm the extent to which criminological theories such as SLT can adequately explain and predict offending behaviours online. Despite several calls in leading IS journals for studies that further our understanding of the motivations of cybercriminals, studies on social engineering attacks and other cyber-offences have mainly been addressed from the perspective of victims. Moreover, although scholars often acknowledge the influence of digital environments and processes on online deception, few have examined how they motivate online offenders. Instead, several studies contend that scammers are mainly motivated by financial rewards. Using data from active AFF scammers and drawing on SLT as a baseline theory, our findings led us to propose CTM. Although the attributes in CTM are inspired by SLT, CTM better accounts for cyber-offences by introducing digitally enabled attributes to SLT’s traditional concepts. Specifically, CTM explains how digital technologies are changing the concepts of learning criminality through criminal socialisations, imitations, definitions, reinforcements, and justifications. Furthermore, the digitally enabled concepts identified in our research add new conceptualisations to SLT and caution IS scholars against adopting criminological theories wholesale because the online context is changing cyber-offenders' motivations and specialised offending knowledge.

References

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.

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology, 30*(1), 47-88.

Akers, R. (2011). Social learning and social structure: A general theory of crime and deviance.

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

Akers, R., & Jennings, W. (Eds.). (2009). *Social learning theory* (J. Millers, 21st Century criminology: A reference handbook ed.) Thousand Oaks: SAGE Publications, Inc.

Akers, R. & Jennings, W. G. (2009). The social learning theory of crime and deviance. *Handbook on crime and deviance* (pp. 103-120) Springer.

Akers, R., & Jensen, G. (2006). The empirical status of social learning theory of crime and deviance: The past, present, and future. *Taking Stock: The Status of Criminological Theory, 15*, 37-76.

Akers, R. L. (1973). Deviant behavior: A social learning approach.

Akers, R. L. (1998). Social structure and social learning. *Los Angeles: Roxbury*

Akers, R. L., & Sellers, C. S. (2004). Criminological theory.

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

Ampratwum, E. F. (2009). Advance fee fraud "419" and investor confidence in the economies of sub-Saharan african (SSA). *Journal of Financial Crime,*

APWG. (2017, Phishing activity trends report. *Anti-Phishing Working Group,*

Arachchilage, N. A. G., & Cole, M. (2016). Designing a mobile game for home computer users to protect against phishing attacks. *arXiv Preprint arXiv:1602.03929,*

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences, 1*(03), 23.

Bandura, A. (1977a). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191.

Bandura, A. (1977b). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191.

Bandura, A. (1986). The explanatory and predictive scope of self-efficacy theory. *Journal of Social and Clinical Psychology, 4*(3), 359-373.

Bandura, A., & McClelland, D. C. (1977). *Social learning theory* Englewood cliffs Prentice Hall.

Benjamin, V., Zhang, B., Nunamaker Jr, J. F., & Chen, H. (2016). Examining hacker participation length in cybercriminal internet-relay-chat communities. *Journal of Management Information Systems, 33*(2), 482-510.

Bernasco, W. (2013). *Offenders on offending: Learning about crime from criminals* Routledge.

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

Burgess, R. L., & Akers, R. L. (1966). A differential association-reinforcement theory of criminal behavior. *Social Problems, 14*(2), 128-147.

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

Button, M., & Cross, C. (2017). Cyber frauds, scams and their victims. Routledge. Provides a good overview of fraudsters, advanced fee frauds etc.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391-408.

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The qualitative report*, *21*(5), 811-831.

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.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review,* 588-608.

Cornish, D. B., & Clarke, R. V. (2016). The rational choice perspective. In *Environmental criminology and crime analysis* (pp. 48-80). Routledge.

Cressey, D. R. (1957). The state of criminal statistics. *NPPA Journal*, *3*(3), 230-241.

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

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Duah, F. A., & Kwabena, A. M. (2015). The impact of cybercrime on the development of electronic business in ghana. *European Journal of Business and Social Sciences, 4*(01), 22-34.

Edwards, M., Peersman, C., & Rashid, A. (2017). Scamming the scammers: Towards automatic detection of persuasion in advance fee frauds. Paper presented at the *Proceedings of the 26th International Conference on World Wide Web Companion,* 1291-1299.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*(4), 532-550.

Feeney, F. (1986). Robbers as decision makers. in (derek B. cornish and ronald V. clarke, eds.), the reasoning criminal: Rational choice perspectives on offending.

Freilich, J. D., & Newman, G. R. (2015). Transforming piecemeal social engineering into" grand" crime prevention policy: toward a new criminology of social control. *The Journal of Criminal Law and Criminology*, 203-232.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the gioia methodology. *Organizational Research Methods, 16*(1), 15-31.

Glaser, D. (1956). Criminality theories and behavioral images. *American Journal of Sociology, 61*(5), 433-444.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report*, *8*(4), 597-607.), 2)

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime.* Stanford University Press.

Gundur, R. V. (2017). Using the internet to recruit respondents for offline interviews in criminological studies. *Urban Affairs Review,* 1078087417740430.

Hartung, F. E. (1965). *Crime, law and society* Detroit: Wayne State University Press.

Hennink, M. M., & Kaiser, B. N. (2020). *Saturation in qualitative research*. Thousand Oaks, CA: Sage Publications Limited.

Holt, T. J., & Graves, D. C. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology, 1*(1), 137-154.

Hutchings, A., & Holt, T. J. (2018). Interviewing cybercrime offenders. 75.

IC3. (2019, Internet crime report.

Isacenkova, J., Thonnard, O., Costin, A., Francillon, A., & Balzarotti, D. (2014). Inside the scam jungle: A closer look at 419 scam email operations. *EURASIP Journal on Information Security, 2014*(1), 4.

Jacobs, B. A., Topalli, V., & Wright, R. (2003). Carjacking, street-life and offender motivation. *British Journal of Criminology, 43*(4), 673-688.

Jacques, S. (2018). Which source possesses the best data on the empirical aspects of criminal events? A theory of opportunity and necessary conditions. *Deviant Behavior*, 1-10. doi:10.1080/01639625.2018.1559635

Jamieson, R., Land, L.P.W., Winchester, D., Stephens, G., Steel, A., Mauruchat, A., Sarre, R. (2012). Addressing Identity Crime in Crime Management Information Systems: Definitions, Classification, and Empirics, Computer Law & Security Review, 28(4):381-395.

Kirk, J., Miller, M. L., & Miller, M. L. (1986). *Reliability and validity in qualitative research* Sage.

Lacey, D., Goode, S., Pawada, J., & Gibson, D. (2020). The application of scam compliance models to investment fraud offending. *Journal of Criminological Research, Policy and Practice*.

Liedtka, J. M. (1992). Exploring ethical issues using personal interviews. *Business Ethics Quarterly*, 161-181.

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.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *Mis Quarterly, 34*(3), 431-433.

Matsueda, R. L. (1988). The current state of differential association theory. *Crime & Delinquency, 34*(3), 277-306.

Miethe, T. D., & Meier, R. F. (1994). *Crime and its social context: Toward an integrated theory of offenders, victims, and situations* Suny Press.

Niiniluoto, I. (1999). Defending abduction. *Philosophy of Science, 66,* S436-S451.

Nyrup, R. (2015). How explanatory reasoning justifies pursuit: A peircean view of IBE. *Philosophy of Science, 82*(5), 749-760.

Office of the Comptroller of the Currency (2022). Types of Consumer Fraud. Types of Consumer Fraud | OCC

Ofulue, C. I. (2010). A digital forensic analysis of advance fee fraud (419 scams). *Handbook of research on discourse behavior and digital communication: Language structures and social interaction* (pp. 296-317) IGI Global.

Onyebadi, U., & Park, J. (2012). 'I'm sister maria. please help me': A lexical study of 4-1-9 international advance fee fraud email communications. *International Communication Gazette, 74*(2), 181-199.

Park, Y., Jones, J., McCoy, D., Shi, E., & Jakobsson, M. (2014). Scambaiter: Understanding targeted nigerian scams on craigslist.

Queensland Police (2022). Advance fee fraud. Advance fee fraud | QPS (police.qld.gov.au)

Ransbotham, S., Fichman, R. G., Gopal, R., & Gupta, A. (2016). Special section introduction—ubiquitous IT and digital vulnerabilities. *Information Systems Research*, *27*(4), 834-847.

Ross, S., & Smith, R. G. (2011). Risk factors for advance fee fraud victimisation. *Trends and Issues in Crime and Criminal Justice*, (420), 1.

ScamWatch. (2021). Scam statistics. Retrieved from https://www.scamwatch.gov.au/scam-statistics

Security Magazine (2021). 5 biggest cybersecurity threats | 2021-02-03

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34*(4), 495-518.

Smith, D. J. (2010). A culture of corruption. Princeton University Press. There is a chapter on Nigerian 419 scammers.

Smith, A. (2009) Nigerian scam e-mails and the charms of capital. Cultural Studies

StoneBrige (2014). A look at different types of Advance Fee Fraud. A look at different types of Advance Fee Fraud - StoneBridge Business Partners (stonebridgebp.com)

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior*, *7*(3), 321-326.

Sutherland, E. (1947). Principles of criminology.

Sutherland, E., & Cressey, D. (1947). Principles of criminology.

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

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in nigeria. *International Journal of Cyber Criminology*, *5*(2)

Tambe Ebot, A. C., & Siponen, M. (2014). Toward a rational choice process theory of internet scamming: The offender's perspective.

Taylor, M., & Quayle, E. (2008). Criminogenic qualities of the internet in the collection and distribution of abuse images of children. *The Irish Journal of Psychology*, *29*(1-2), 119-130.

Topalli, V. (2005). When being good is bad: An expansion of neutralization theory. *Criminology*, *43*(3), 797-836.

Topalli, V., Dickinson, T., & Jacques, S. (2020). Learning from criminals: Active offender research for criminology. *Annual Review of Criminology, (3)*, 189-215.

Topalli, V., & Nikolovska, M. (2020). The future of crime: How crime exponentiation will change our field. *The Criminologist, 45*(3), 1-8.

Urquhart, C. (2013). *Grounded theory for qualitative research: A practical guide* Sage.

U.S. Securities and Exchange Commission (2022). Advance Fee Fraud. Advance Fee Fraud | Investor.gov

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems, 15*(3), 320-330.

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems, 17*(11), 759-783. Retrieved from https://search.proquest.com/docview/1851172057?accountid=11363

Warr, M. (2002). *Companions in crime: The social aspects of criminal conduct* Cambridge University Press.

Webster, J., & Drew, J. M. (2017). Policing advance fee fraud (AFF) Experiences of fraud detectives using a victim-focused approach. *International Journal of Police Science & Management*, *19*(1), 39-53.

Whittaker, J. M., & Button, M. (2020). Understanding pet scams: A case study of advance fee and non-delivery fraud using victims' accounts. *Australian & New Zealand Journal of Criminology, 53*(4), 497-514.

Wikström, P. H. (2006). Individuals, settings, and acts of crime: Situational mechanisms and the explanation of crime. *The Explanation of Crime: Context, Mechanisms and Development*, 61-107.

Wincup, E. (2017). *Criminological research: Understanding qualitative methods*. Sage.

Wright, R., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems, 27*(1), 273-303.

Wright, R., & Topalli, V. (2013). Choosing street crime. *The oxford handbook of criminological theory* (pp. 461-474) Oxford University Press.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research, 25*(2), 385-400.

Yar, M. (2005). The novelty of 'Cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.

Yingling, J., & McClain, M. B. (2015). *Snowball sampling, grounded theory, and theoretical sampling: Roles in methamphetamine markets* SAGE Publications, Ltd.

APPENDIX

Table 1. Overview of some AFF scams

Type	Description
Beneficial fraud or inheritance scam	The scammer indicates that he/she has inherited a huge sum of money (e.g., USD 13 million). The reason could be the death of a parent or spouse. However, the scammer says the money is held at a bank and the scammer cannot retrieve it, as he/she does not have the fees that the bank needs to release the funds. The bank will not deduct the fee from the savings. Consequently, the scammer needs the recipient's help; if the recipient advances the fee, she/he will be rewarded (e.g., half of the total sum).
Lottery scam	The scamming message informs the recipient that he/she has won a lottery. The message states the date the recipient won, the amount, and the date by which the prize must be collected. The message also emphasizes that the lottery took place through a random computer ballot system of hundreds of thousands of names and email addresses. The money has been cleared for collection. However, the winner must advance a relatively small amount as a processing fee. Again, the fee cannot be deducted from the amount won.
Pet scam	The scammer advertises a puppy. The puppy is free but is in Africa. When a user replies to the offer, the scammer provides more photos, explains why it is being offered for free, and tells the recipient what needs to be done before the puppy can be shipped (i.e., payment for vaccines, transportation costs, and customs, etc.).

Romance scam	The scammer (a man) claims to be a woman seeking love. If necessary, the scammer will pay a female friend to sit in for a video call. Once trust is established, the scammer begins to make requests for money (e.g., to pay for an accident, visa documentation, a sick parent).
Investment scams	Investment scams employ social engineering techniques that promise individuals big payouts, quick money, or guaranteed returns on their investments in exchange for a small upfront payment or "investment" from the individual.
Craigslist scam	The scammer advertises merchandise for sale. Typically, there will be little information about the merchandise itself other than the fact that the scammer wants to sell it urgently. When a buyer makes contact, the scammer will send natural-looking pictures of the merchandise. The scammer emphasizes residence in a different city to avoid a physical meeting and proposes a legitimate-sounding escrow service for the transaction, knowing the buyer will not bother to verify that the company's identity is stolen. The scammer requests that the money be sent through Western Union.

Table 2. Summary of AFF scamming research

Authors	AFF scamming research
Abia et al. (2010)	This study examined the extent to which students are involved in AFF scamming in Cameroon and the existing intervention measures. The authors administered a questionnaire to 500 middle students to ascertain their awareness of internet crimes and fraud generally and knowledge of friends who engaged in scamming. They reported that over half of participants knew a friend who was involved in scamming and about 95% made had scammer friends for financial reasons. They concluded that scamming is a contributing factor to school dropout and bad for the country's image.
Akinladejo (2007)	This conceptual paper discussed trends and legislative issues involved in AFF scamming with a focus on scamming in the Caribbean context. The author concluded that while efforts are focused on combatting drug trafficking and money laundering, international and efforts should focus on AFF scamming. Author also associates AFF as a problem of greedy individuals with a "get rich quickly" syndrome.
Adogame (2009)	This study examined 150 scam letters to describe how scamming variations emerged. The findings located the economic and sociopolitical crises that contributed toward Nigerian scams to the late 1979s. The study also reported how scams became more complex and sophisticated to attract and deceive people around the globe.
Ampratwum, (2009)	This conceptual study examined the nature and causes of Nigerian "419" fraud because little work has investigated its impact on investment and economic development in sub-Saharan Africa. Focusing the discussion on the political and historical context of AFF in Sub-Saharan Africa, the author concluded that scamming has a negative effect on economic development as people are Africa to invest in the continent because of high crime. The author recommends transnational collaboration to control AFF scamming.

Aigbovo, (2019)	This study reviewed Nigerian economic and financial crime statutes. The review uncovered that Nigerian economic and financial crime statutes have been evolving over the years to address crimes such as AFF scamming which is assumed to have originated from Nigeria and is covered by Section 419 of the Nigerian penal code.
Atkins & Huang (2013)	Authors suggest that advance fee fraud is so-called because the scheme requires a victim to pay the scammer in advance with the promise of receiving rewards later. AFF fraudsters use persuasive communication to skillfully manipulate their victims into an emotionally vulnerable state.
Atta-Asamoah (2010)	This is a research commentary to describe the process of using AFF scamming from West Africa to deceive individuals worldwide. The commentary associates the proliferation of AFF scamming to unemployment and desperation and contends that African scammers are “young economic and social desperadoes” (p. 107) from different African countries. The process of AFF scamming deception is described as involving scouting and harvesting through emails, relationship building, and requesting money. The internet is described as facilitating document falsification, identity theft, and money laundering and AFF scamming has a negative impact on legitimate business from West Africa.
Boateng et al. (2008)	This study investigated the prevalence of AFF scamming (i.e., ‘sakawa’ in Ghana) and measures used to address it. The study focused on the forms of cybercrime common in Ghana and how Ghana is addressing cases of AFF scamming specifically. The study collected data from 40 respondents including bank personnel, police investigators, legal practitioners, and internet fraud victims. Their findings suggested that scamming awareness remains low, local law enforcement lacks the technical know-how, and scammers are young people with technical computer knowledge. They identified unemployment, the quest to get rich quickly, gullible, and greedy foreigners, lack of legislation, and commitment from banks as additional antecedents of scamming.
Burrell (2008)	Arguing that scamming practices in West Africa involve narratives about political turmoil, corruption, poverty, violence, and personal tragedy, this study examined how internet scammers are complicit in promoting dramatic, stereotyped representations about Africa and Africans. Drawing from sociological theories, this study suggests that scammers are recreating and manipulating representations of Africa (in terms of poverty and high unemployment) to a mainly Western audience in exchange for financial gain.
Cassandra (2018)	Arguing that frauds are underreported, this study examined online fraud victims who reported their victimization to law enforcement. The findings identified two motivations for reporting, namely, to achieve a feeling of justice and to be altruistic (i.e., reporting to protect others).
Chang, (2008)	Authored argued that AFF scamming is an epidemic and describes it as involving persuading victims to advance relatively small amounts of money with the expectation of realizing a much larger return. AFF scammers persuasive tactics rely on false claims that they are Nigerian officials, royalty, or businesspeople because they want the recipients’ help in transferring money out of Nigeria. In exchange, victims are promised a share in the proceeds as compensation for their help. Using six cases of AFF messages, the author reported that scammers exploit victims’ bounded rationality and automatic behaviours based on the following influence techniques: authority and expert power, impersonation and misrepresentation, urgency, scarcity, and reciprocity.
Chawki, (2009)	Author describes AFF scamming as a form of “419” which comes from section 419 of the Nigerian criminal code. The specific criminal code deals with a complex list of frauds, cheating, stealing, falsification, impersonation, counterfeiting, forgery, and fraudulent representations.

Cukier et al., (2008)	Authors posit that AFF messages, or “Nigerian letters” are a specific form of spam that deceive recipients into making advance payments in exchange for some future promise. Fraudsters frame these advance payments as “fees” necessary to procure a much bigger sum of money.
Dobovsek et al. (2013)	This literature review study applied quantitative and qualitative techniques to understand how AFF scams work. They reported that AFF scams are not declining, and scammers are using spamming techniques and targeted messaging to that target recipients based on their interests. This means AFF scams are a global concern as no country is immune from scammers’ tactics.
Dion (2010)	This study examined AFF scams from the perspectives of Machiavellianism and narcissism. Following an analysis of 100 AFF (lottery, humanitarian gifts, business opportunities, gold/diamond) scam letters, they reported that AFF letters reflect a Machiavellian/narcissistic approach of human behavior and morality.
Edwards, Peersman, & Rashid (2017)	According to authors, AFF involves promising victims, wealth, gifts, prizes, or employment in exchange for a small advance payment. Once a victim acquiesces to fraudsters request by making an advance payment, the fraudsters collect the money and then disappear.
Holt & Graves (2007)	Authors contend that AFF messages come from individuals who want victims to help them with moving large sums of money, typically out of Nigeria. They further describe how AFF scams initially appeared as handwritten letters before morphing into email messages with the advent of digital technology.
Igun (2008)	This study reviewed the literature on cybercrime with an emphasis on AFF fraud in Nigeria to describe the techniques scammers are adopting. The paper concludes that the ease of accessing the internet, online anonymity, socioeconomic conditions of poverty, corruption, and unemployment, and weak laws against cybercrime are responsible for the prevalence of AFF scamming in Nigeria.
Isacenkova, Thonnard, Costin, Francillon, & Balzarotti, (2014)	According to the author, 419 scams are also known as Nigerian scams and they are a popular form of fraud used by fraudsters to trick individuals into paying a certain amount of money under the promise of a future, larger payoff.
Noel Otu (2013)	Arguing that Nigerian scammers are diversifying their AFF tactics, this conceptual study investigated why Nigerian “419 syndicates have begun engaging in kidnapping for ransom. The paper argued that AFF “419” is no longer as lucrative as it used to be. Consequently, kidnapping for a ransom is an unintended consequence of decades of the rich preying on the poor.
Onyebadi & Park (2012)	According to authors, AFF known simply as 419 is a scheme designed by fraudsters who claim to have lucrative business, humanitarian, or philanthropic related dealings. The fraudsters promise the victim large sums of money in exchange of a small initial investment.
Ofulue (2010)	Author describes AFF as the act of deceiving individuals or potential clients into making advance payments or giving away their valuables in exchange for a substantial profit or returns. They also note that AFF which originated from Nigeria and is also referred to as “Nigerian Advance Fee fraud” or “419”, is based on Section 419 of the Nigerian Criminal code that prohibits the fraud.
Park, Jones, McCoy, Shi, & Jakobsson (2014)	According to the authors, AFF scamming also known more commonly as “Nigerian scams” or “419 scams” is a prevalent form of online fraud that causes financial loss to individuals and businesses. They highlight how victims suffer negative emotional or psychological impact.
Ross & Smith (2011)	The authors contend that AFF scams offer individuals business deals with wealthy individuals or dignitaries who need help in large sums of money from a foreign country in exchange for a commission. They further note that AFF scams involve several variations, such as asking that victims pay fees to

	receive lottery winnings, paying fees to receive an inheritance or a prize, and paying advance money to establish personal relationships.
Whittaker and Button (2020)	This study uses from a volunteer group’s database that focuses on preventing pet scamming, a specific type of AFF scamming to shed light on the strategies scammers employ to maximise their chances of deceiving online buyers. Relying on victim’s accounts, the study reported that scammers employ the technique of impersonation with authentic-looking websites, urgency to pressure victims into making quick decisions, and anonymous payment methods to avoid detection.
Webster and Drew (2017)	This article argued that the transnational nature of AFF scamming that takes place online presents challenges for enforcing traditional deterrence measures. Using semi-structured interviews with police detectives who investigate scamming attacks, the findings highlight the changes of designing effective enforcement strategies to reduce the certainty and severity of AFF scamming.
Whitty and Buchanan (2016)	This article examined the psychological impact of online romance scams to understand its impact on the victims. They reported victims of these crimes experienced “double hit” financial and relationship losses. Most victims tried coping with their losses through denial which results in additional victimization.

The core components of SLT

Differential association: The first core concept of SLT is a direct outgrowth of Sutherland’s (1947a) theory; differential association serves the social context within which the other three concepts (see below) function. It describes how exposure to criminal attitudes, values, norms, and behaviors following socialization processes with offenders influence a person’s attitude and behavior regarding crime (Akers, 2011; Sutherland & Cressey, 1947). Exposure to criminal attitudes and behaviors may be direct or indirect and typically occurs within primary (family and peers) and secondary (e.g., church, school, and mass media) reference groups (Akers & Jensen, 2006). However, SLT emphasizes that peer–friendship and family primary group are the most important, providing more immediate contexts that promote or discourage deviant, delinquent, or conforming behaviors. Further, SLT posits that associations that last longer, occupy a disproportionate amount of the individuals' time, occur frequently, and involve intimate or close friends and family have the greatest influence on behavior (Akers & Jennings, 2009b). Unsurprisingly, the criminological literature has consistently reported that delinquent peers influence delinquent behavior (Matsueda, 1988; Warr, 2002).

Definitions: Definitions are the positive or negative orientations, attitudes, justifications, rationalizations, and excuses used to characterize a behavior as more right than wrong (positive definitions), more good than bad (negative definitions), or more justified than unjustified (neutralization definition) (Akers & Jensen 2006). SLT views attitudes (Burgess & Akers, 1966; Sutherland, 1947), beliefs (Gottfredson & Hirschi, 1990), orientations (Sutherland, 1947b), and neutralizations or justifications (Akers & Jennings, 2009; Sykes & Matza, 1957) as dimensions of definitions. Exposure to criminal definitions may also lead a person to imitate a behavior after observing it in others, especially when the observed person is seen as benefitting from the behavior (Bandura, 1977). Consistent with this, empirical research on computer crime suggests that individuals who hold definitions favoring the violation of computer laws and norms are more likely to commit computer deviance (Skinner & Fream, 1997). In context of social engineering attacks, offenders' manifest favorable definitions through schemes that influence, manipulate, and deceive online users into performing actions, such as submitting personal and sensitive information or, in the current paper, providing advance payments for nonexistent merchandise.

Imitation and Emulation: Imitation involves observing and modeling the behaviors of others. Models can be real (e.g., humans) or symbolic (present in books, films, or online). Akers notes that imitation may be more important in the beginning phase of criminality as opposed to the continuation or desistance phases (Akers, Ronald L., 1998). Imitation is influenced by several factors, including the characteristics of the model, whether observers see the model experiencing reinforcements from their actions (e.g., display signs of pleasure), and if it takes place in an environment that encourages a models' behaviors (Bandura, 1977b; Bandura, 1986). In SLT, imitation alone is inadequate for explaining the acquisition and maintenance of criminal behavior. Although SLT contends that the learning process is not limited to the process of imitation, its principal learning mechanisms incorporate a combination of differential reinforcement and imitation (observational learning). Reinforcements and imitations influence the cognitive definitions and behaviors that serve as discriminative stimuli for the behavior. Online, the potential to virtually meet and observe models is theoretically limitless. Offenders may also use digital artifacts to perform multiple roles, influence a large number of unsuspecting online users with much more frequency while disguising their true identities, locations, or intentions.

Differential reinforcement: Differential reinforcement refers to positive and negative outcomes or reactions that are expected to result from an act (Akers & Sellers, 2004). The differential reinforcement process operates through four key modalities: positive reinforcement, negative reinforcement, positive punishment, and negative punishment. According to SLT, peer approval serves as positive reinforcement for crime when a criminal act increases an individuals' status, wealth, or pleasant feelings. Negative reinforcement increases the likelihood of repeat behavior if the perpetrator can avoid an unpleasant outcome, such as being apprehended after committing a criminal act. Positive and negative reinforcers emphasize the rewards of a behavior while deterrence emphasizes punishment or avoidance. In addition, positive and negative punishments can either increase or decrease the likelihood that a behavior is repeated. Positive punishment is a painful or unpleasant experience resulting from a behavior, such as being caught for scamming, whereas negative punishment is the removal of benefits following a deviant or delinquent act (Akers, Ronald L. & Jennings, 2009a). Differential reinforcement posits that the greater the rewards and likelihood of avoiding formal (e.g., legal deterrence) or informal (e.g., parental or peer disapproval) punishment, the more likely a behavior will be repeated. Therefore, Akers' SLT also subsumes the concept of deterrence into differential reinforcement. Deterrence theory predicts that perceived certain and severe punishment is likely to discourage a person from engaging in a criminal behavior (D'Arcy, Hovav, & Galletta, 2009). For scamming, this means previous financial scamming successes or non-financial successes (e.g., the thrill from deceiving people online or assuming false identities) combined with online anonymity may increase scamming activity.

Interview Protocol Form

Introductory Protocol

Thank you for agreeing to participate. My name is ***** I am a researcher in Finland. I am researching cybercriminals and victims. I want to talk with you because I am doing research on internet scamming, and I understand that you are a scammer. Let me just run through a few things. To facilitate note taking, I would like your permission to audio tape our conversations today. Your answers to these questions will be kept confidential, that is, only the researchers involved directly in this project will have access to your answers, and your answers will eventually be destroyed after the data analysis. I should also emphasise that your participation is voluntary, and you may stop at any time if you feel uncomfortable. This interview has been planned to last about 35 minutes and no longer than 60 minutes. During this time, there are a couple questions that I would like to cover with you.

Interview Questions

1. Do you have questions that I can clarify before we start?
2. Please indicate your age group: 18-24; 25-34; 35-44; 45-and above

3. What is your level of education?
4. Tell me how you were introduced to scamming until you eventually became a scammer?
5. Tell me about the friends who introduced you into scamming.
6. What do you do as an internet scammer?
7. Could you describe a typical scamming process?
8. How would you refer to victims?
9. Can you describe your best scamming experience?
10. What are the challenges of operating as a scammer?
11. Are you concerned about getting caught?
12. Have you ever thought of quitting?

Subsequently, we asked questions relating to the role of information technology and social learning theory. These questions arose after we analysed the data, realised a social learning process, chose SLT as our theoretical base, and also found that we needed to focus on the role of IT from an information systems perspective.

1. What technologies do you use for scamming? Describe the different technologies and how you use them during a scamming process.
2. How did you learn from your friends; how did you learn from cybercafes; what did you learn on your own?
3. Have you ever done or thought of doing FtF scamming in the physical environment?
4. What are the advantages of doing scamming online as opposed to doing it FtF?
5. Would you continue practicing scamming if the internet ceased to exist?

Follow-up questions were often based on how subjects responded to the questions and emphasised subjects' reasons for their actions. Follow-up questions are not included in this protocol.