Toward a Rational Choice Process Theory of Internet Scamming: The Offender's Perspective

Research-in-Progress

Tambe Ebot Alain Claude
University of Jyväskylä
Jyväskylä, Finland
alcltamb@student.jyu.fi

Mikko Siponen
University of Jyväskylä
Jyväskylä, Finland
Mikko.t.siponen@jyu.fi

Abstract

Internet fraud scam is a crime enabled by the Internet to swindle Internet users. The global costs of these scams are in the billions of US dollars. Existing research suggests that scammers maximize their economic gain. Although this is a plausible explanation, since the idea of the scam is to fool people to send money, this explanation alone, cannot explain why individuals become Internet scammers. An equally important, albeit unexplored riddle, is the question of what strategies Internet scammers adopt to perform the act. As a first step to address these gaps, we interviewed five Internet scammers in order to develop a rational choice process theory of Internet scammers' behavior. The initial results suggest that an interplay of socioeconomic and dynamic thinking processes explains why individuals drift into Internet scamming. Once an individual drifts into Internet scamming, a successful scam involves two processes: persuasive strategy and advance fee strategy.

Keywords: Internet scamming, Internet scammers, Internet crime, interpretive research, process theory

Introduction

Internet fraud scams in which scammers fool a buyer or an investor in an online transaction are a well-known threat, enabled by the Internet. In 2013 alone, the losses from Internet scamming were estimated at US$12.7 billion (Ultrascan 2013). Although Internet scammers are known to operate largely from the West African region (Burrell 2008), the targets of Internet scammers are around the globe (Akinladejo 2007). The highest number of Internet scam complaints were from the United States, Canada, the United Kingdom, Australia, and India (IC3 2010). The act of an Internet scam has two sides: 1) the Internet scammer as the offender and 2) the victim as the target. For the former, researchers should understand not only the causes and reasons for becoming an Internet scammer, but also the strategies that Internet scammers adopt to perform the scam. For the latter, the focus should be on why individuals react to Internet scams. In other areas of information systems (IS) security, such as computer abuse (D'Arcy et al. 2007; Straub 1990) and employee compliance with information security procedures (Siponen & Vance 2010, 2014), the focus has been on understanding the offender (1), not on the potential victims of computer abuse or policy violations (2). However, in the case of Internet scamming, previous IS researchers focused on the victims (2), by understanding their behaviors, mainly under the "phishing" label (e.g., Moody et al. 2011; Wright & Marett 2010). More specifically, researchers examined why people fall for phishing attacks (Wright et al. 2014).

For Internet scamming, only one study examined the act from the Internet scammers' perspective (1) and concluded that Internet scammers are motivated by economic gain (Burrell 2008). This is no surprise as the act of Internet scamming is all about fooling individuals to send money to Internet scammers. At the same time, this finding tells us little about how one becomes an Internet scammer. Indeed, many individuals motivated by economic gain, do not become Internet scammers. Hence, although Internet scammers may be motivated by economic gain, such explanations alone cannot be the whole story of how one becomes an Internet scammer. An equally important, albeit unexplored, riddle is the question of what strategies Internet scammers use to perform Internet scamming. To summarize, it is not known how one becomes an Internet scammer, what strategies internet scammers use to design Internet scams, and why they perform Internet scams. Our broad research questions seek to understand: *how and why Internet scammers plan and execute Internet fraud scams?*

In this research-in-progress paper, we report a research project that contributes to these two open issues by developing a specific rational choice theory (RCT) of Internet scamming from the offender's perspective. More specifically, the theory contributes to the IS literature by adding three processes to RCT theory, which are specific for Internet scamming. The first process explains how one becomes an Internet scammer. Through the two other processes, the theory explains how Internet scammers operate and change their tactics in order to successfully deceive targets constantly.

The rest of the paper is organized as follows. In the next section, we review the literature on Internet scamming and point out the research gap, to which our RCT theory will contribute. In the third section, we discuss the RCT approach to theorizing and explain our motivation for building a rational choice process theory of Internet scammers' behavior. We then explain our methodological approach, and finally, we present the preliminary results of our rational choice process theory of Internet scammers' behavior.

Internet Scamming and Previous Work

Internet scamming messages are similar to other deceptive messages (Wright et al. 2014; Xiao & Benbasat 2011): They are sent out in a deliberate attempt to mislead individuals (Burrell 2008). The messages involve misrepresentation (i.e., telling a falsehood about a specific situation) (Burrell 2008). The general form of scamming messages dates back to the late 16th century, and the messages were sent through postal mail (Burrell 2008). However, some characteristics of Internet scamming distinguish it from scamming activities conducted offline. Internet scamming occurs through computer-mediated channels, such as

email, bulletin boards, chat rooms, and social media. In one approach to Internet scamming, Internet scammers spam email accounts with tales about pets available for adoption, gold discovered in Ghana or Nigeria, fortunes from dead relatives, and so on. In another approach, Internet scammers post a carefully designed on certain websites and social media in the hope that Internet users will react (Atta-Asamoah 2009, p. 109). The focus of this study is on the latter approach. An examination of Internet scamming messages suggests Internet scammers want to deceive individuals into making advance fee payments, in exchange for the merchandise (e.g., pets, and cash crops such as, coffee beans) they claim to have for sale (Herley 2012). Evidence from Internet scamming messages also suggest that such payments are framed as costs of logistics (i.e., freight, flights, quarantine, or insurance) necessary before the merchandise can be authorized by customs officials for shipping (Salifu 2008). In reality, Internet scammers do not possess the merchandise they advertise; and they have no intention of acquiring and/or supplying them. Thus, Internet scamming involves misrepresentation and persuasive story-telling (Burrell 2008).

Even though Internet scamming has been traditionally associated with the West African region, Internet fraud scams have become a global problem (Ampratwum 2009). As such, adequately addressing it requires the concerted efforts of researchers, governments, and civil society (Westby 2003; Broadhurst 2006). For example, due to scamming activities, banks require documentation (e.g., a letter of credit, authorization to sell) as proof that a supplier (the scammer) is not a scammer, before effectuating payment requests from their customers. Recent reports show that Internet scamming is growing at a rate of five percent per year, with scamming rings spreading worldwide (Ultrascan 2010). Although Nigeria continues to top the list of resident scammers', countries such as the United States, China, Canada, Ghana, and France have experienced an increase in Internet scamming activities (Ultrascan 2010). Although the threats posed by computer crime have been studied in several different contexts (Willison & Siponen 2009; Moody et al. 2011; Johnston & Warkentin 2010; Wright & Marett 2010; Vance & Siponen 2012; Xu et al. 2013), Internet scammers have received less attention.

In terms of examining scammers' behavior, Burrell (2008) conducted an ethnographic study in Ghana, by interviewing Internet scammers, Internet café owners, Internet users, and relatives of Internet scammers, to understand the assumed relationship between networking technologies and socio-economic benefits. Based on this information, Burrell reported that Internet scammers misrepresent themselves online in order to attract targets and utilize persuasive strategies to unite their interests (e.g., economic gain) with those of their targets. Internet scammers assume identities they believe will increase their chances of deceiving a target and making money out of him or her. Other studies have not directly examined scammers. By examining a catalog of internet scam emails, Herley (2012) investigated why certain Nigerian scammers indicate that they are from Nigeria. Herley's (2012) idea was that advance fee frauds are associated with Nigeria in particular, and the West African region in general. Herley speculated that scammers wanted to distinguish gullible and non-gullible users before they invest time and effort in persuasion. However, in the study by Herley (2012), Internet scammers first spam email users with tales of wealth, or the death of relatives, in the hope that an individual will show interest and respond. The Internet scammers we study in this research-in-progress use a different variant of scamming in which they design and place ads online and on Facebook. In other Internet scamming studies meanwhile (e.g., Boateng et al. 2011; Chang 2008), researchers have focused on Internet scam victims and Internet scam emails.

In summation, only study on Internet scamming directly examined the act of performing Internet fraud scams from Internet scammers' perspective; and the conclusion was that Internet scammers are motivated by economic gain (Burrell 2008). Alas, this finding tells us little about *how* one becomes an Internet scammer, what strategies Internet scammers utilize when performing Internet fraud scams, and how Internet scammers evolve their strategies when the strategies utilized are unsuccessful? An equally important question not answered in prior research is: *why* do Internet scammers perform their behaviors? We contribute to these unaddressed issues, by developing a specific rational choice theory of Internet scamming, from the perspective of offenders. Next, we describe a rational choice approach to theory building.

Rational Choice Approach to Theory Building

Rational choice theories (RCTs) have a long history in disciplines such economics, sociology, political science, and criminology (Akers 1990). Because different RCT theories have been developed in different disciplines and sometimes within different contexts within those discipline, various approaches exist. For example, when Cornish and Clarke (1986) developed an RCT in criminology, it was developed to explain a specific form of street crime, e.g., burglaries in specific neighborhoods (de Haan & Vos 2003). Nevertheless, many of the RCTs in different disciplines share a common core assumption on which the specific theory is based. They assume different variations of rationality, from full rationality, bounded rationality, and procedural rationality to social rationality. Theories with full rationality assume that individuals have complete knowledge about their decision alternatives, the probabilities of their outcomes, and their consequences. In turn, theories of bounded rationality assume that the decision makers do not have complete knowledge, are limited by time and their own cognitive abilities, and will choose a course of action that they believe will maximize their benefits (Cornish & Clarke 1986; Akers 1990). Finally, many RCT theories assume that individuals have preferences ranging from selfishness, opportunism, egoism, and linked-utility to solidarity. A selfishness assumption, for example, implies an individual will readily break rules (e.g., cheat) to maximize his or her benefits. In most RCTs, individuals are regarded as self-interested agents with the ability to make judgments about achieving subjectively defined goals (Akers 1990). Other types of RCTs have also been proposed (Gigerenzer & Selten 2001; Hodgson 2012; McCarthy 2002).

IS researchers have adopted economic and criminal versions of RCTs (e.g., Bulgurcu et al. 2010; Willison & Siponen 2009). When adapting theories from other disciplines to an IS setting, it is important to pay attention to the context by refining the theory based on the context (Hong et al. 2013). Similarly, several IS researchers (e.g., Orlikowski & Iacono 2001; Weber 2003) have emphasized specificity, in terms of the information technology (IT) artifact in IS theory development. Following this idea, this research-in-progress is an attempt to develop a specific rational choice process theory of Internet scamming, by focusing on the offenders' perspective. The research methodology is described in the next section.

Research Methodology

This research-in-progress adopts an interpretive approach (Walsham 1995). An interpretive approach is useful in understanding the perceived reality of Internet scamming from the offender's (Internet scammers) perspective. The credibility and generalizability of this study are therefore context dependent (ibid). The preliminary data was collected through semi-structured interviews with professional Internet scammers operating in Cameroon. All interviews were audio-recorded, and the interview data served as the empirical input for this preliminary data analysis. Similar to most West African countries, Cameroon is currently experiencing an economic downtown, high corruption, and high unemployment among the age group that is the most susceptible to becoming Internet scammers. Nevertheless, Internet scamming has been legislated as a criminal activity in Cameroon. However, this has not deterred some individuals from engaging in Internet scam frauds.

It was difficult to recruit and interview Internet scammers. We were unable to approach the scammers directly, since many were scared that we worked for Interpol. To recruit scammers for this study, we relied on a local acquaintance in Cameroon. His job included contacting successful and experienced Internet scammers, explaining the purpose of the research, and assuring them that the interviews are anonymous. After they agreed to participate, the field researcher further explained the purpose of the study and further reassured the interviewees of their anonymity. Thus far, five professional Internet scammers have been interviewed. These interviews took place in March 2014 in Cameroon. The interviews lasted 60 minutes on average, and each interviewee was encouraged to discuss in as much detail as possible, the historical context in which they became Internet scammers, how they plan their Internet scams, and why their scamming plans are sometimes successful and other times unsuccessful. We examined what drove them to start using the Internet, what they initially did on the Internet, what they knew about scamming before they became scammers, how and where they first heard about scamming, how they plan (design) and execute (set into motion) successful scamming strategies, how the Internet affects the processes, and so on.

Among those interviewed, there was credible evidence from reliable sources that their Internet scamming activities have yielded success on several occasions, and on several occasions, the scammers have been apprehended by law enforcement officers. To analyze the preliminary interview data, we used an adaptation of grounded theory procedures (Urquhart 2013). We used open coding at the sentence level to label the data and performed selective coding by grouping the relevant relationships among the open codes (Glaser 1978; Urquhart et al. 2010). The choice of open codes and the groupings of selective codes are informed by our research questions (Urquhart 2013). The themes that emerge from the selective codes are integrated with the base theory, i.e., RCT (Cornish & Clarke 1986) adopted in this study. Rational choice theory emerged as a relevant theoretical lens from the interviews; for example, the whole idea of the Internet scamming is economic benefit, and Internet scammers use different rational strategies to perform their scam.

Toward a Rational Process Theory of Internet Scamming

Preliminary Findings from the Qualitative Analysis

The preliminary process model (Figure 1) shows the process that led the interviewees to Internet scamming and how they prepare and execute their Internet scamming strategies.

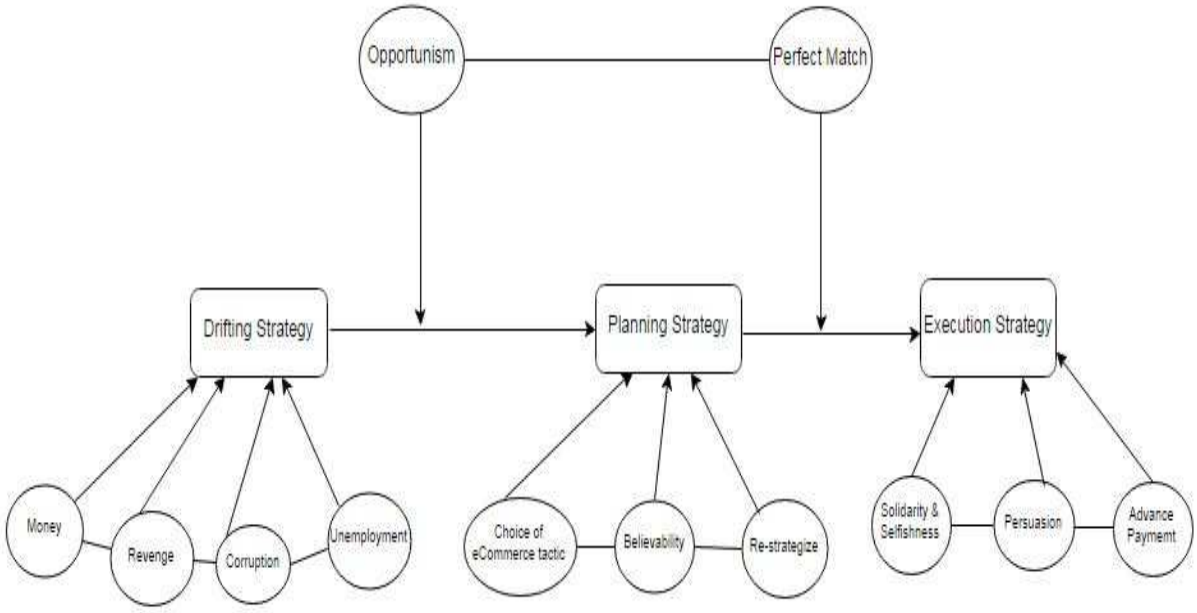

Figure 1. Process Model of a Successful Internet Scamming Strategy

Figure 1 also explains how the Internet scammers prepare their Internet scamming strategies, and determine whether the strategies will be successful. It shows how Internet scammers combine interacting strategies and transitional factors.

Table 1. Empirical and Theoretical Constructs and Definitions		
Empirical Constructs	***Empirical Construct Definitions***	***Assumptions in Rational Choice Theory***
Process 1:	Drifting strategy explains Internet scammers'	RCT uses rationalizations to

Drifting strategy	rationality as a combination of experiences (marginalization and disenchantment), giving rise to a set of factors: money, revenge, corruption, unemployment.	explain why people become, criminals, for example, using factors such as a need for money, social status, and peer pressure (de Haan & Vos 2003).
Process 2: Planning strategy	Planning strategy explains Internet scammers' rationality and provides a new understanding of how opportunistic behavior can be expressed in a RCT context, i.e., in terms of choice of ecommerce tactic, believability in designing Internet scamming messages, and re-strategizing.	Rational choice suggests opportunism, selfish, egoism, linked utility, and solidarity as preference assumptions (Gächter 2013).
Process 3: Execution strategy	Execution strategy explains why a successful Internet scamming recipe is affected by a preference for selfishness. It provides a new understanding of the selfishness preference in RCT by describing selfishness in terms of new factors. These factors are tactics that Internet scammers use to achieve a successful Internet scam: multiple identities (hiding under the cloak of Internet anonymity), expressing solidarity to achieve selfishness.	Rational choice preference assumptions range from tangible and intangible resources to physical well-being and social well-being (Gächter 2013). However, these preferences are expressed at a high conceptual level, with little context provided.
Process Theory of Internet scamming	A process theory explains Internet scammers' recipe for scamming individuals as a dynamic phenomenon. It also explains why a chain of strategies evolve into a successful recipe for Internet scamming.	
Opportunism	Opportunism is a transitional factor. It is explains why Internet scammers choose Internet scamming, i.e., because it is an efficient means for reaching their goals (revenge and personal financial reward). Efficiency in opportunism means Internet scammers can reach millions of potential targets with a few Internet scam messages posted on websites and Facebook.	Opportunism implies that parties in an interaction deliberately cheat in order to increase their own benefits (Wittek et al. 2013).
Perfect match	Perfect match is another transitional factor. It explains why Internet scammers can move to the process of deploying a successful Internet scam execution strategy. That is, they groom their targets through multiple interactions, and if their plans match the targets' demands, then the scammers move to the execution process.	RCT of criminal behavior (Clarke 1992) assumes that offenders mostly choose their victims (in street crimes and burglaries, for example) randomly.

How They Became Internet Scammers: The Drifting Strategy

The drifting strategy explains how Internet scammers ended up being professional Internet scammers. In rational choice theorizing, individuals use rationalizations to justify their behaviors, e.g., burglars (de Haans & Vos 2003). The preliminary interview data provided a specific understanding of these rationalizations from Internet scammers' perspective. The data suggests that interviewees who have worked as Internet scammers for more than 10 years (aged between 30 and 38 years) drifted into Internet scamming as a means of revenge, i.e., payback. Namely, they wanted financial rewards as payback for

their revenge. They felt their attempts to gain lawful employment or start up their own legitimate businesses had failed because of exploitative buyers and endemic corruption. The Internet scammers justify their move to scamming through their experiences of disenchantment, arising from the marginalization and exploitation they have suffered. Internet scamming was the most opportunistic means to reach that objective. The preliminary results also suggest that the younger generation of Internet scammers (aged between 20 and 24 years) drifted into scamming because they were inspired by the luxury lifestyles of the older scammers. Internet scamming was an opportunistic means to reach their goals: it is cost effective. Even though they claim to sell merchandise, the main costs they incur include: cost of time spent on the Internet, time spent designing an Internet scam advertisement, and cost of using the Internet. In previous RCT research on burglars, it was found that they have no rational decision-making processes (Cromwell & Olson 2003). Rather, their burglaries were opportune (e.g., open garage door, open windows), the offender had previously visited the house for legitimate reasons (e.g., delivery person). Offenders' decisions, according to Cromwell & Olson (2003) were not conscious rational choice processes. This is the perspective of the RCT of crime (Cornish & Clarke 1986).
In contrast, our results suggest that, while Internet scammers initially chose Internet scamming as an opportunistic means to reach their goals, they effectuate a rational decision-making process in how they plan their Internet scams after they transitioned into professional Internet scammers.

How to Plan an Internet Scam: The Planning Strategies

The planning strategy explains how, after drifting into Internet scamming, Internet scammers plan, design, and execute the first phase of their scamming deception strategy. In planning an Internet scamming deception strategy, Internet scammers are careful to ensure that they can achieve their objectives of opportunism, in which they lie, cheat, and deceive individuals. RCT assumes that individuals have preferences, and often choose the preferences that maximize their own self-interests (McCarthy 2002). The rational choice approach of crime suggests that offenders often lack complete knowledge about their targets and tactics; as such, they exhibit partial rationality which associated with rudimentary planning (Cornish & Clarke 1986). Past research suggests that offenders, e.g., in street crimes and burglaries, choose their targets randomly (de Haan & Vos 2003) .

Our preliminary data suggests that Internet scammers seriously consider which Internet scamming tactic to adopt and plan for, e.g., choosing between spamming email users with their scams and posting the Internet scams on websites and Facebook. Internet scammers express rationality in their ecommerce tactic; that is, they rationally choose to post their scam advertisements on websites and Facebook so that only interested individuals will choose to contact them. Their goal is to achieve a perfect match—the right candidates for Internet scamming. This is more likely to happen if the advertisements are posted on websites and on Facebook; and if they are designed to appear believable. Herley (2012) reported that Nigerian 419scammers broadcast that they are from Nigeria to make their Internet scamming recipe successful. Furthermore, our interviewees reported that should the need arise, they re-strategize, by lowering the selling price of the merchandise, in order to not lose "the customer", that is, the target. A request by a target for a lower selling price, is often a strong signal of intent from a customer. A successful planning strategy recipe therefore targets a perfect match and sends a signal that this act is not a scam, and that matches is successful.

How They Execute the Internet Scam: The Execution Strategy

The advance payment strategy explains how Internet scammers try to meet their objective of successfully scamming individuals. Rational choice theorizing assumes that if individuals are constrained by time and/or complete knowledge, then the assumptions of full rationality will not hold (Akers 1990; Cornish & Clarke 1986; de Haan & Vos 2003). Our interviews suggest that the time to completion of a successful Internet scam depends on how the Internet scammers execute their tactical plans, as well as on how their targets react to those plans. Nevertheless, the Internet provides scammers with anonymity; thus, they can create multiple identities in executing their deception plans. Given their preference for selfishness (rational choice; selfish assumption, e.g., Wittek et al. 2013), their execution strategy also has to be persuasive. Targets need to be persuaded to make advance payments. For this, they use a rational assumption of solidarity (ibid) in which they pretend to show concern for their targets, by requiring that the full selling price will be paid only after the target receives the merchandise. By showing solidarity,

Internet scammers can meet their preference for selfishness, by persuading targets to make advance payments. The advance payments are based on fraudulent documentation the scammers prepare, and which show that insurance and freight charges must be paid before the merchandise can be authorized to leave the country by the customs authorities. An advance payment is the financial benefit or gain of Internet scamming; the payment is also a means for exercising revenge.

Conclusive Discussion

The preliminary results suggest that Internet scammers drift into Internet scamming due to the interplay of a socioeconomic process and a dynamic thinking process. Once an individual drifts to the business of Internet scamming (process 1), a successful scam involves two processes: persuasive strategy (process 2) and advance fee strategy (process 3). Future theory development must focus on chasing further specifics of these strategies. For drifting (process 1), the goal is to build an explicit stage-theory or process theory, which contains critical stages or triggers, which explains with specific details, how people drift into Internet scamming. Understanding the steps or triggers for becoming a scammer will help society design early intervention strategies, which can hopefully prevent people from turning to the business of scamming. The need for such information is critical, because an early intervention that prevents people from becoming Internet scammers would be much more effective than educating users to avoid scammers' tactics. Especially, as our results show, the scammers revise their tactics if they are not effective. Having said that, further understanding of the strategy processes 2 and 3 is nevertheless helpful for providing guidelines on how potential victims of Internet scamming can avoid scamming.

As for study limitations, the Internet scammers interviewed for this research-in-progress paper operate in West Africa. The findings regarding the drifting strategy may not hold for scammers outside this region. Our sample of five professional scammers is not yet representative, and further interviews are required to obtain additional information and reach the point of saturation.

References

Akers, L. 1990, "Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken," (81:3), pp. 653-676.

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

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

Broadhurst, R. 2006, "Developments in the Global Law Enforcement of Cyber-Crime," *Policing: An International Journal of Police Strategies & Management* (29:3), pp. 408-433.

Burrell, J. 2008, "Problematic Empowerment: West African Internet Scams as Strategic Misrepresentation." *Information Technologies & International Development* (4:4), .

Chang, J. J. 2008, "An Analysis of Advance Fee Fraud on the Internet," *Journal of Financial Crime* (15:1), pp. 71-81.

Clarke, R. 1992, "Situational Crime Prevention: Successful Case Studies," .

Cornish, D., and R. Clarke. 1986, "Rational Choice Approaches to Crime," *The Reasoning Criminal: Rational Choice Perspectives on Offending*pp. 1-6.

Cromwell, P., and J. N. Olson. 2005, "The Reasoning Burglar: Motives and Decision-Making Strategies," *In their Own Words: Criminals on Crime (an Anthology)*pp. 42-56.

D'Arcy, J., A. Hovav, and D. Galletta. 2009, "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

de Haan, W., and J. Vos. 2003, "A Crying Shame the Over-Rationalized Conception of Man in the Rational Choice Perspective," *Theoretical Criminology* (7:1), pp. 29-54.

GACHTER, S. 2013, "Rationality, Social Preferences, and Strategic Decision-Making from a Behavioral Economics Perspective," *The Handbook of Rational Choice Social Research*pp. 33.

Gigerenzer, G., and R. Selten. 2001, "Rethinking Rationality," *Bounded Rationality: The Adaptive Toolbox*pp. 1-12.

Glaser, B. G. 1978. *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*, Sociology Press Mill Valley, CA.

Herley, C. 2012. "Why do Nigerian Scammers Say they are from Nigeria?" .

Hodgson, G. M. 2012, "On the Limits of Rational Choice Theory," *Economic Thought* (1:1), .

Internet Crime Complaint Center (IC3). 2013; 2012. "Internet Crime Report," .

Johnston, A. C., and M. Warkentin. 2010, "Fear Appeals and Information Security Behaviors: An Empirical Study." *MIS Quarterly* (34:3), .

McCarthy, B. 2002, "New Economics of Sociological Criminology," *Annual Review of Sociology*pp. 417-442.

Orlikowski, W. J., and C. S. Iacono. 2001, "Research Commentary: Desperately Seeking the "IT" in IT research—A Call to Theorizing the IT Artifact," *Information Systems Research* (12:2), pp. 121-134.

Salifu, A. 2008, "The Impact of Internet Crime on Development," *Journal of Financial Crime* (15:4), pp. 432-443.

Siponen, M., and A. Vance. 2014, "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations," *European Journal of Information Systems* (23:3), pp. 289-305.

Siponen, M., and A. Vance. 2010, "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487.

Straub Jr, D. W. 1990, "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Ultrascan-AGI. 2010. "Advanced Fee Fraud Statistics 2009", accessed (2nd May 2014), http://www.ultrascan-agi.com/

Urquhart, C. 2013. *Grounded Theory for Qualitative Research: A Practical Guide*, Sage.

Urquhart, C., H. Lehmann, and M. D. Myers. 2010, "Putting the 'theory'back into Grounded Theory: Guidelines for Grounded Theory Studies in Information Systems," *Information Systems Journal* (20:4), pp. 357-381.

Vance, A., and M. T. Siponen. 2012, "IS Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End User Computing (JOEUC)* (24:1), pp. 21-41.

Walsham, G. 1995, "Interpretive Case Studies in IS Research: Nature and Method," *European Journal of Information Systems* (4:2), pp. 74-81.
Weber, R. 2004, "Editor's Comments: The Grim Reaper: The Curse of E-Mail," *MIS Quarterly* (28:3), pp. iii-xiii.
Westby, J. R. 2003. "International Guide to Combating Cybercrime," .
Willison, R., and M. Siponen. 2009, "Overcoming the Insider: Reducing Employee Computer Crime through Situational Crime Prevention," *Communications of the ACM* (52:9), pp. 133-137.
Wittek, R., T. Snijders, and V. Nee. 2013. *The Handbook of Rational Choice Social Research*, Stanford University Press.
Wright, R. T., M. L. Jensen, J. B. Thatcher, M. Dinger, and K. Marett. 2014, "Research Note-Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance," *Information Systems Research* (25:2), pp. 385-400.
Wright, R. T., and K. Marett. 2010, "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived," *Journal of Management Information Systems* (27:1), pp. 273-303.
Xiao, B., and I. Benbasat. 2011, "Product-Related Deception in e-Commerce: A Theoretical Perspective," *MIS Quarterly* (35:1), pp. 169-196.
Xu, Z., Q. Hu, and C. Zhang. 2013, "Why Computer Talents Become Computer Hackers," *Communications of the ACM* (56:4), pp. 64-74.