JYVÄSKYLÄ STUDIES IN COMPUTING
259

Alain Claude Tambe Ebot

Explaining Two Forms of Internet Crime from Two Perspectives

Toward Stage Theories for Phishing and Internet Scamming

JYVÄSKYLÄN YLIOPISTO

JYVÄSKYLÄ STUDIES IN COMPUTING 259

Alain Claude Tambe Ebot

Explaining Two Forms of Internet Crime from Two Perspectives

Toward Stage Theories for Phishing and Internet Scamming

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen Lea Pulkkisen salissa
tammikuun 26. päivänä 2017 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, Lea Pulkkinen hall, on January 26, 2017 at 12 o'clock noon.

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2017

Explaining Two Forms of Internet Crime from Two Perspectives

Toward Stage Theories for Phishing and Internet Scamming

JYVÄSKYLÄ STUDIES IN COMPUTING 259

Alain Claude Tambe Ebot

Explaining Two Forms of Internet Crime from Two Perspectives

Toward Stage Theories for Phishing and Internet Scamming

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2017

Editors
Marja-Leena Rantalainen
Department of Mathematical Information Technology, University of Jyväskylä
Pekka Olsbo, Ville Korkiakangas
Publishing Unit, University Library of Jyväskylä

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-6954-7

URN:ISBN:978-951-39-6954-7
ISBN 978-951-39-6954-7 (PDF)

ISBN 978-951-39-6953-0 (nid.)
ISSN 1456-5390

Jyväskylä University Printing House, Jyväskylä 2017

ABSTRACT

Tambe Ebot, Alain Claude
Explaining two forms of Internet crime from two perspectives: toward stage theories for phishing and Internet scamming
Jyväskylä: University of Jyväskylä, 2017, 116 p.
(Jyväskylä Studies in Computing
ISSN 1456-5390; 259)
ISBN 978-951-39-6953-0 (nid.)
ISBN 978-951-39-6954-7 (PDF)

The two studies in this dissertation examine two pervasive and common forms of Internet crimes from two different perspectives: (1) phishing from the victims' perspective and (2) Internet scamming from the offenders' perspective. For the former, previous phishing research is based on models that assume that fixed or static factors explain or predict people's reasons for complying with phishing emails. These models assume that the reasons for complying with phishing emails are the same across individuals and across time. However, we argue that, whereas the act of clicking on a phishing email is the same across time for phishing victims, the reasons for complying are not the same. We address this problem with interview data from actual victims of phishing emails. The overall findings show how differences in process attributes lead individuals to comply for different reasons. We further theorize why phishing victims reside in one of two stages and propose a tailored approach to reducing phishing.

For the second issue, despite making headline news and the estimated cost in the billions annually, scamming research is at an exploratory stage. Focusing on why individuals become scammers, the academic research on scamming has suggested (1) monetary rewards, (2) structural problems, and (3) affordable Internet access. We argue, however, that individuals in need of money, experiencing poverty and unemployment, and having affordable Internet access, do not become criminals. To address these problems, we interviewed actual Internet scammers. Regarding why individuals become scammers, we suggest that money is because it is needed to socialize, to enjoy an extravagant lifestyle, and to remain or become financially independent. Further, we contribute to finding how individuals become scammers by identifying three stages that respectively explain the initial progression into scamming, the specific choice of scamming and the role of the Internet, and the reasons scammers persist in scamming. We theorize these findings using criminology literature and show that neither the dispositional nor situational criminological theories can adequately explain the proclivity toward scamming and the act of practicing Internet scams. We make suggestions for practice.

Keywords: phishing, scamming, Internet crimes, dispositional crime theories, situational crime theories, interpretive research, stage theorizing

Author Alain Claude Tambe Ebot
Faculty of Information Technology
University of Jyväskylä
Finland
alcltamb@jyu.fi

Supervisor Professor Mikko Siponen
Faculty of Information Technology
University of Jyväskylä
Finland

Reviewers Dr. Robert Willison
Business School
Newcastle University
United Kingdom

Professor Gurpreet Dhillon
School of Business
Virginia Commonwealth University
USA

Opponents Professor Volkan Topalli
Department of Criminal Justice & Criminology
Georgia State University
USA

Dr. Petri Puhakainen
Security Advisor
Silverskin Information Security Oy
Finland

DEDICATION

To my mother, Ebot Margaret Eneke, for her largess and selfless dedication to my success.

To my wife, Therese, for coping with my moods and long absences from home.

To my children, Abigail and Kylden, who are still very young. I hope you will always persevere through whatever obstacles you encounter as you grow older and never relent or allow others make you relent in the pursuit of your dreams.

ACKNOWLEDGEMENTS

This dissertation culminates the end of four arduous, yet exciting years for me as a PhD student. Yet, it only seems to be the beginning of my academic career. I am really thankful to Prof. Mikko Siponen for giving me the opportunity to be a PhD student and for acting with diligence toward my academic and occasional personal needs. I am grateful for his emphasis on only developing manuscripts for top journals. I am also grateful that Mikko provided whatever resources he thought were necessary to improve the quality and chances that the manuscripts in this dissertation will be published in top IS journals, for example, presenting and discussing my research to leading IS scholars and journal editors. Now that I can see more clearly, I am grateful that he constantly emphasized: "Shoot to the moon. Even if you miss, you'll land among the stars." I am also very grateful to him and to the Department of Computer Science and Information Systems for financing my many research field and conference trips.

I heartily thank my opponents Professor Volkan Topalli and Dr. Petri Puhakainen for their time and the helpful comments. I am thankful to my reviewers, Dr. Robert Willison and Prof. Gupreet Dhillon for their comments. I thank Drs. Mari Karjalainen, Aggeliki Tsohou, Andy (Nan) Zhang, and Markus Salo for providing comments on earlier versions my research. I am thankful to the administrative staff for assisting me with any administrative problems. I am also grateful to the CS & IS staff for their conviviality. I equally thank former and current members of the Cameroonian community in Jyväskylä and my friends across Finland for their wonderful company.

Jyväskylä 26.01.2017
Tambe Ebot, Alain Claude

FIGURES

TABLES

CONTENTS

1 INTRODUCTION

1.1 Research background and research questions

This dissertation addresses two important types of Internet crime from two perspectives: (1) phishing from the victims' perspective and (2) Internet scamming from the offenders' perspective. The Internet has evolved into a complex, dynamic, and globally interconnected digital and information infrastructure (Maughan, 2010). Its ubiquity has made online behaviors, such as ecommerce, communicating (e.g., via email, instant messaging, and social media), and Internet browsing part of people's daily routines. In addition to underpinning every aspect of society and providing communication and development, it has also become a minefield of crimes, perpetuated on a global scale (Lee, 2015).

Among common Internet crimes, phishing represents a major form of online identity theft, and Internet scamming is a major problem for ecommerce. The International Telecommunication Union estimated that almost 3.2 billion people used the Internet in 2015 (International Telecommunication Union, 2015), representing almost half of the world's population. In behavioral information security literature, users are often regarded as the weakest security link (Hu et al., 2012; Crossler et al., 2013). While several information systems (IS) security studies have examined Internet crimes, such as phishing, from the victims' perspective (Wright et al., 2014; Wright & Marett, 2010; Downs et al., 2006) and attempts have also been made to understand the motivations of hackers from the offenders' perspective (Abbasi et al., 2010; Hu et al., 2011; Young et al., 2007), academic studies on Internet scamming are almost nonexistent in the mainstream IS journals and conferences. Even though Internet scammers continue to make headline news due to their activities, IS researchers have only alluded to scamming in calls for more black-hat studies (Crossler et al., 2013; Mahmood et al., 2010; Lee et al., 2015). However, a few academic studies on scamming have been published (Burrell, 2008; Adomi & Igun, 2008; Salifu, 2008) in other outlets and disciplines.

In general, while a few Internet crime academic studies have used actual hackers (Young et al., 2007; Hu et al., 2011) and actual Internet scammers (Burrell, 2008), we are not aware of any that have used actual phishing victims. Although a number academic studies have improved our understanding of why people comply with phishing emails (Wang et al., 2012; Vishwanath et al., 2011), research on Internet criminals (e.g., hackers and scammers) is at an exploratory stage with limited sample sizes (Crossler et al., 2013). While there is a need to study actual victims of Internet crimes, there is also an urgent need for rigorous empirical studies on actual Internet criminals. These shortcomings could be addressed through inductive studies and/or through studies that draw on criminological theories. Regardless, gaining rich understandings of Internet crime victims and offenders could lead to new theory development in the IS security field that can also affect other related disciplines. In two empirical studies, this dissertation addresses two shortcomings in the extant academic literature on Internet crimes.

1.2 Summary of the dissertation

Although this dissertation addresses Internet crimes from two perspectives, the two studies in the dissertation were not conducted to understand the relationship between phishing and Internet scamming. These are two independent studies conducted to improve our understanding of Internet crimes from two separate perspectives. I briefly introduce the two studies below.

1.2.1 How dispositional differences affect peoples' reasons for complying with phishing emails: Toward a stage theory

This study addresses the problem in the literature that people are deceived by phishing emails for the same reasons. In other words, it tackles the assumption that the reasons dispositional factors explain or predict being deceived by phishing activity are the same across phishing victims. For example, according to past research, people become victims because they lack security experience (Wright & Marett, 2010), they focus disproportionately on the phishing message (Vishwanath et al., 2011), and they are overconfident (Wang et al., 2016). We argue that, although the act of clicking on a phishing link is the same for all phishing victims, the reasons for clicking will be different because they are affected by individual attributes, such as online behaviors, prior security knowledge, and experiences that affect people's behaviors in different ways. In practice, this means that the current approach to recommending the same anti-phishing programs for all victims might not be an effective strategy. In this study, we adopt an inductive, grounded theory approach and rely on interviews with actual victims of phishing emails. The research question is:

How do differences in people's Internet behaviors affect their reasons for complying with phishing emails?

A major contribution from this study is showing that the differences resulting from dispositional attributes (individuals' online behaviors and experiences) affect how they process and comply with phishing emails differently. We theorize that phishing victims reside in one of two stages. Residence at a particular stage is affected by the differences stemming from how they process phishing. Further, the source of the differences between Stage 1 and 2 victims are explained in four processes.

In Process 1, the nature of email and Internet use is used to explain the difference between victims residing in Stage 1 from the victims residing in Stage 2. Stage 1 victims use behaviors that are influenced by the trend and the need to connect and chat with friends. Thus, they perceive a problem in a phishing email simply as a problem that should be fixed, otherwise their browsing might be interrupted. In contrast, Stage 2 victims engage in creating, storing, and sharing personal photos, information, and secrets. Consequently, a phishing email makes them concerned about their online behaviors (personal/business transactions), primary email accounts, and online contacts and relationships.

In Process 2, prior security encounters, explains the difference between Stage 1 and 2 victims. Because of their attributes at Process 1, Stage 1 victims cannot identify a security threat and a solution to the threat. A phishing email is simply a problem with a solution. In contrast, Stage 2 victims can identify a security threat, but not a solution to the threat. Thus, they focus on consequences of compliance and noncompliance. However, they become confused because they have doubts about the right course of action. These doubts emerge because they are aware of conflicting security messages, which in turn affect their confidence.

Process 3 is only applicable to victims in Stage 2 because the residents in Stage 1 have not yet reached this stage. Process 3, information security and privacy concerns, is used to explain how Stage 2 victims fear the negative consequences of a breach and how that clouds their judgment. Finally, Process 4, encounters with phishing email, explains how Stage 1 and 2 victims were deceived by phishing emails based on the outcomes in the previous processes. In practice, these differences mean that anti-phishing recommendations should be tailored for different Internet users based on their stage of experience, knowledge, and online behaviors.

1.2.2 How one becomes an Internet scammer: Toward a stage theory

This study is based on face-to-face semi-structured interviews with actual Internet scammers. The main objective is to explain how individuals become scammers. However, the findings also extend to why money motivates people to commit scams and why scammers persist in scamming. Internet fraud scamming is a common and effective form of computer crime in which scammers use misrepresentation and persuasive communication in online interactions to swindle Internet users. The global cost of these scams is in the

billions of US dollars. Extant academic Internet scamming research has proposed three main reasons that individuals become Internet scammers: (1) monetary rewards, (2) structural problems (corruption, unemployment, and poverty), and (3) cheap Internet. We argue, however, that several individuals who like monetary rewards and are experiencing structural problems and enjoying inexpensive Internet do not become scammers. Therefore, the existing explanations do not tell the whole story about why one would become an Internet scammer. Moreover, extant scamming research does not explain how one becomes an Internet scammer.

To address these problems, we ask: How does one become an Internet scammer? First, the findings from this study explain why money motivates people to become scammers. Although past research has identified money as a motivator, it does not explain why money motivates individuals to choose to become scammers. We report that money is needed to socialize, enjoy the extravagant lifestyle of scammers, and for individuals to remain or become financially independent. Second, we explain how individuals become Internet scammers, suggesting that it occurs in three stages that are affected by different factors. Stage 1 explains that individuals' previous histories (pre-scamming events and relationships) produce negative emotions that motivate the movement toward scamming. Stage 2 explains why individuals specifically become scammers. The identified reasons include associations with scammers, lifestyle preferences, a desire to become or to maintain financial independence, and the characteristics of the Internet. Finally, Stage 3 explains why scammers do not quit, in other words, why they persist in scamming. The identified reasons include the use of justifications, deterrence measures, and use of a hired third party (a pickup). We relate these findings to extant scamming and IS security literature. We also relate these findings to the relevant dispositional and situational criminological theories. We report that none of the extant dispositional crime theories that explain the proclivity toward criminality (e.g., social learning theory) can adequately explain why people become scammers. We also report that, although situational crime theories (e.g., routine activities theory) were developed to explain why criminal acts occur, they cannot adequately explain why scamming occurs because they can neither explain the role of the offender nor the role of the computer-mediated environment in criminality. The implications for practice are discussed.

1.3 Publication status

As already mentioned, this dissertation consists of two studies (shown as follows), which are either under review with a journal or will be submitted to a journal for review:

I. Ebot, T. A., Siponen, M. (2017). How dispositional differences affect peoples' reasons for complying with phishing emails: toward a

stage theory. Under review at Journal of the Association of Information Systems.

II. Ebot, T. A., Siponen, M. (2017). How does one become an Internet scammer? toward a stage theory. Unpublished manuscript.

Tambe Ebot Alain is the first author of the articles listed in this dissertation and did the majority of the related work, including gathering the data for both studies. Prof. Mikko Siponen, acting as my doctoral advisor, provided overall guidance and valuable comments for the two articles included in the dissertation. The earlier versions of these articles were accepted and published as follows:

III. Ebot, T. A., Siponen, M. (2014). Shame: A New Approach to Phishing Victimization. *JAIS* (Journal of the Association of Information Systems) Theory Development Workshop, ICIS Auckland, New Zealand.

IV. Ebot, T. A., Siponen, M. (2014). Toward a Rational Choice Process Theory of Internet Scamming: The Offender's Perspective. Thirty Fifth International Conference on Information Systems, Auckland (2014).

The earlier articles (III and IV) have been significantly improved in the form of articles I and II, respectively. This dissertation, therefore, is solely based on the articles I and II.

2 STUDY I. HOW DISPOSITIONAL DIFFERENCES AFFECT PEOPLES' REASONS FOR COMPLYING WITH PHISHING EMAILS: TOWARD A STAGE THEORY

2.1 Summary of Study I

This study examines how differences in individuals' prior online behaviors and experiences affect being deceived by a phishing email. Previous phishing research is based on models that assume that fixed or static factors explain or predict people's reasons for complying with phishing emails. For example, according to past phishing research, when people receive emails threatening their university email accounts, their reasons for complying include experiential attributes (e.g., limited security knowledge) and phishing attributes (e.g., urgency cues). These reasons are assumed to affect the victims' decisions to comply in the same manner, and they are also assumed to remain the same across time. We argue, however, that only the act of clicking on a phishing link is the same for all phishing victims and remains the same across time. The differences resulting from individuals' diverse online behaviors, experiences (e.g., differences in security knowledge), and their different reasons for their online behaviors suggest that people are likely to comply for different reasons.

We address this problem by interviewing actual victims of threatening phishing emails. Our findings show how differences in process attributes lead individuals to comply for different reasons. We theorize that phishing victims reside in one of two stages. Residence at a particular stage is affected by differences stemming from how they process phishing. We highlight the differences between Stage 1 and 2 residents through the following processes: the nature of email and Internet use (Process 1), prior encounters with security (Process 2), information security and privacy concerns (Process 3), and encounters with phishing emails (Process 4). For example, Stage 1 victims can neither recognize a security problem nor identify and utilize a security solution.

In contrast, Stage 2 victims can recognize a security problem; however, they cannot extrapolate to understand and utilize the correct security solution. Thus, Stage 1 victims become phishing victims because they focus on the phishing messages' authenticity, legitimacy, and security appeal. In contrast, Stage 2 victims comply with phishing emails because their inadequate security knowledge makes them confused, doubtful, and lacking in confidence. Thus, Stage 2 victims adopt a mistaken protective motivation behavior regarding their information security and privacy. Our findings highlight the limitations of a one-size-fits-all approach to understanding why people comply with phishing emails. For practice, we recommend a tailored approach that accounts for individual differences when designing and implementing anti-phishing recommendations.

2.2 Introduction

Phishing represents a major form of online financial and identity theft (Wright, Jensen, Thatcher, Dinger, & Marett, 2014). Phishers (perpetrators of phishing emails) attempt to steal online users' personal and sensitive information through phishing attacks (Harrison, Svetieva, & Vishwanath, 2016). While exact phishing costs are hard to obtain, estimates put the global costs of phishing against individuals and organizations in the billions of US dollars (RSA Security LLC, 2014). Typically, there are two types of phishing emails: (1) phishing emails with threats (e.g., "your account has been breached," "your account will be deactivated in 24 hours," or "Urgent: account security update") (2) phishing emails with benefits/rewards (e.g., "you have won" or "congratulations"). Of the two types of phishing emails, the first type has been the most used in phishing research. On one hand, behavioral security researchers investigating why people comply with phishing emails have focused primarily on the phishing email design and appearance (e.g., Vishwanath, Herath, Chen, Wang, & Rao, 2011) and phishers' use of influence techniques (Wright et al., 2014). On the other hand, researchers have studied individual attributes that affect compliance with phishing emails, for example, computer self-efficacy, security awareness, perceived risk (Wright & Marett, 2010), lack of attention, and limited phishing knowledge (Harrison et al., 2016).

Typically, the findings from past research suggest that phishing emails elicit compliance by utilizing influence techniques to deceive Internet users possessing particular attributes, such as limited security knowledge and low computer self-efficacy (Wang, Herath, Chen, Vishwanath, & Rao, 2012; Wright & Marett, 2010). Although previous research has improved our understanding of the factors likely to increase or decrease compliance with phishing emails, we highlight one important issue that requires further study.

Past phishing research assumes that victims of phishing emails comply for the same reasons. This assumes a phishing compliance mechanism that is based on explanatory or predictor factors that are fixed or stable across different

individuals. For example, when different people receive phishing emails threatening their university accounts, past research has suggested that the reasons that factors such as lack of attention or security knowledge affect their decisions to comply are the same for everyone. We argue that although the act clicking on a phishing link is the same for all phishing victims, differences stemming from individuals' attributes (e.g., years of experience, knowledge, and online behaviors) means their reasons for complying cannot be the same. Thus, a person's reasons for complying – the process by which they interpret and form judgments about a phishing email – will be different. In practice, this means that the current approach to recommending the same anti-phishing programs for all victims might not be an effective strategy.

Process models are suitable for explaining such differences because they can conceptualize different reasons for performing an action in stages or phases (Schwarzer, 2008a). Accordingly, we adopt a process approach to answer the following research question: *How do differences in people's Internet behaviors affect their reasons for complying with phishing emails?* This study is based on data obtained through face-to-face semi-structured interviews with actual victims of threatening phishing emails. Our findings show how differences in process attributes lead individuals to comply for different reasons. We theorize that phishing victims reside in one of two stages. Residence at a particular stage is affected by the differences stemming from how they process phishing.

2.3 Background and Literature Review

This study is motivated by the past assumption in phishing research that phishing victims' reasons for complying with phishing attacks are the same. Because the individual attributes that are known to influence compliance are unlikely to be the same for every victim, we argue that different people will have different reasons for complying. We choose a process approach to address this problem because process research can better account for scenarios in which the reasons are changing (Schwarzer, 2008a). Methodologically, this is an interpretive research based on the inductive process (Rowlands, 2005); that is, we did not go into the field to collect data with specific theories in mind. Our sole intent was to understand why recipients of threatening phishing emails comply with the emails. In the following subsections, we present overviews of phishing research, its relationship with information security and privacy concerns, and finally, process models.

2.3.1 Phishing Emails

Phishing messages are sent with the intent to mislead recipients to accept a falsehood and to perform a specific action (Wright et al., 2014). The success of phishing emails is attributable to several factors, including the legitimate appearance of the phishing messages, the use of authentic or undisputed

sources (e.g., Jagatic, Johnson, Jakobsson, & and Menczer, 2007) and individuals' lack of anti-phishing training and security education (Kumaraguru et al., 2009). Some of the factors that influence a recipients' perception that a phishing message is authentic include the source of the phishing email, its professional look and feel, and the absence of grammar or spelling errors (Vishwanath et al., 2011; Wang et al., 2012).

As email recipients have become more aware and suspicious of global and reputable organizations sending out emails that contain misspellings, phishers have evolved their tactics by designing phishing emails that appear believable (Wright et al., 2014). Thus, updated versions of phishing emails are of high quality and are often hard to distinguish from legitimate emails. Phishing emails are designed to communicate trust, credibility, and authenticity (Vishwanath et al., 2011; Jakobsson, 2007). Further, an important aspect of phishing design is to steal users' personal information. Phishers hope that users who focus on the primary purpose of their interaction, such as ecommerce, chatting, or emailing, are unlikely to pay attention to deceptive cues or security warnings about a phishing attempt (Alsharnouby, Alaca, & Chiasson, 2015).

2.3.2 Past Phishing Research

To inform the design of improved anti-phishing education and awareness programs, researchers have approached phishing in four complementary ways: (1) automatic phishing detection whereby phishing attacks are blocked before they reach the user, (2) security indicators whereby security toolbars are designed to warn users about a potential phishing site (Abbasi, Zhang, Zimbra, Chen, & Nunamaker Jr, 2010), (3) anti-phishing education (Kumaraguru et al., 2007; Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010), and (4) understanding why users are susceptible to phishing (Wang et al., 2012). This study falls within this fourth category.

Past phishing research suggests that phishers take advantage of how people process information to manipulate them into compliance; this research has mainly focused on understanding what makes phishing messages appear authentic and why individuals comply with phishing emails. Researchers and practitioners presume that an understanding of why people comply with phishing emails can lead to the design of phishing education and training programs aimed at reducing phishing compliance (Kumaraguru et al., 2009; Downs, Holbrook, & Cranor, 2006). Table 1 (in appendix 1) summarizes the main findings and the theoretical explanations that past phishing studies have found as reasons for phishing victims' behaviors.

Summarizing, the findings indicate that phishing victims do not engage in systematic processing (Vishwanath et al., 2011; Wright et al., 2014), which involves cognitive thinking and elaboration to make decisions (Wright et al., 2014). Because systematic information processing enables individuals to consider more inputs and to think more carefully, past phishing research indicates that people who perform systematic processing are more likely to detect discrepancies and deception cues (i.e., spelling and grammar errors and

the email source) in phishing emails (Wang et al., 2012). Researchers have also suggested that people with high computer self-efficacy (Wright & Marett, 2010) and prior phishing exposure (e.g., through education and training; (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010) are more likely to elaborate and make detailed assessments about a messages' authenticity.

Drawing on psychological theories (e.g., elaboration likelihood model in the phishing context), researchers have proposed that systematic processing occurs through elaboration (Vishwanath et al., 2011). Elaboration enables individuals to make conscious connections between the information in the phishing message and their prior knowledge. People who engage in the process of elaboration are more likely to comprehend, learn, retain, and recall than those who do not (Cacioppo, Petty, Kao, & Rodriguez, 1986).

Instead, several phishing studies attribute the act of complying with phishing emails with a lack of security knowledge, phishing education, and training (e.g., Kumaraguru et al., 2009). Drawing on psychological theories, researchers have suggested that people become phishing victims because they engage in peripheral information processing (Workman, 2008). Whereas systematic processing encourages elaborative analysis of email content, peripheral processing does not encourage elaboration. Due to peripheral processing, people focus on persuasive elements of a message, such as the perceived credibility, likeability, and attractiveness of the message (Miller, 2004).

Phishing researchers consider peripheral processing to be motivated by involvement, "the perceived relevance of a particular message or event to an individual" (Vishwanath et al., 2011p. 580; Zaichkowsky, 1985). Accordingly, phishing messages that are perceived as relevant are more likely to elicit compliance when individuals focus on the elements of urgency, fear, and threat (Wang et al., 2012). In several controlled experiments involving university students who were educated about phishing, researchers consistently reported that subjects were misled into compliance by personal involvement, source authenticity, and the legitimate appearance of the phishing emails (Moody, Galletta, Walker, & Dunn, 2011; Wright & Marett, 2010). Although threatening phishing emails elicit compliance by claiming a persons' information is at risk, previous researchers on phishing (empirical or theoretical) have overlooked the role of information security and privacy concerns in individuals' decisions to comply with phishing emails.

2.3.3 Information Security and Privacy Concerns

Although phishing attacks are a major threat to peoples' information security and privacy, past phishing researchers do not address how information security influences compliance with phishing emails. Information security seeks to ensure the confidentiality, integrity, and availability of information (Siponen, 2006). The means of achieving these goals include defending information against any unauthorized access, use, disclosure, modification, perusal, inspection, recording, or destruction. People often practice information security

to defend their personal information from an intentional or unintentional danger (Bélanger & Crossler, 2011). Phishing attacks are also associated with information privacy breaches (Afroz & Greenstadt, 2011; Davinson & Sillence, 2010). Information privacy concerns refer to the desire of individuals to control or have some influence over the data about themselves (Belanger, Hiller, & Smith, 2002; Bélanger & Crossler, 2011).

Researchers have studied privacy concerns in terms of the collection and use of personal information. Results indicate that individuals lower their privacy concerns if they perceive a certain degree of control over the collection and use of their personal information (Dinev & Hart, 2004; Xu, Dinev, Smith, & Hart, 2008). Even though researchers found that people prefer control over their information, they also found that some people will put aside such concerns for small rewards (Xu et al., 2008). Yet, by all indications, privacy concerns remain a major concern for most individuals.

2.3.4 Process Models

Variance research and process research are the two research approaches adopted in the information systems (IS) field (Markus & Robey, 1988; Newman & Robey, 1992). Phishing research has traditionally relied on variance models to explain the relationship between individual and phishing attributes. The assumptions concerning variance research are different from those that concern process research. Theories such as the theory of deception and the interpersonal deception theory, as used in phishing studies (Wang et al., 2012; Wright & Marett, 2010), suggest that individuals rely on their past experiences to recognize deception. They do this by noticing and interpreting inconsistencies in phishing factors, for example, wrong sender addresses and uncharacteristic errors in an email from a reputable organization.

In phishing research, the explanatory or predictor factors that are proposed as reasons that people comply with phishing emails are assumed to be fixed in the sense of meaning the same thing for all phishing victims. This is typical of variance models, and consequently, variance-based studies cannot model situations in which the same factors have different explanations for different people performing the same behavior (Schwarzer, 2008a). Instead variance models assume that behavioral changes occur in a linear fashion and make recommendations based on a "one-size-fits-all" approach (Schwarzer, 2008a). Thus, variance studies exclude qualitative differences influencing people with different attributes performing the same behavior, for example, due to differences in years of experience or online behaviors.

By contrast, stage theories often comprise fixed factors in the sense that each stage/process has its own core explanatory or predictor factors. Stage theories are a subset of process theories, and movements from one stage to another lead to new explanatory or predictor factors (Van de Ven & Huber, 1990). Stages are developed to help understand how behaviors change and how interventions can be tailored to best serve the needs of different individuals or groups (Schwarzer, 2008b). Stage theories further assume that different factors

influence transition or movement through a sequence of discrete stages (Sutton, 2005). Recommendations based on stages should consider the different stages and their respective predictive or explanatory factors. Accordingly, a recommendation for practice, for example, should be different for individuals in different stages (Sutton, 2005; Weinstein, 1988). The stage or process approach is deemed valid if its recommendations are more useful when they are tailored to unfold in stages (Schwarzer, 2008a).

2.4 Research Approach

Following past interpretive studies in which researchers have empirically examined the interpretations of key actors (Orlikowski, 1993; Vannoy & Salam, 2010), this study similarly uses the interpretations of victims of phishing emails as key actors to understand how individuals become phishing victims. According to Klein and Myers (1999), through interpretive research, IS researchers can understand human thought and action in diverse contexts. Because people create their own realities, the researcher is expected to interpret these realities in terms of what they mean to the observed people (Lee, 1991).

In phishing research that focuses on how or why people become phishing victims, the key actors are the victims of phishing. In such a scenario, it is important to understand who the victims are and the process by which they interpret and choose to comply with the phishing emails. Interpretive researchers assume that actors actively create their own reality (Isabella, 1990). What is interpreted and theorized is the subjects' understanding of their own actions (Lee & Hovorka, 2015).

Thus, understanding how one becomes a phishing victim is based on how the victims' experiences affect how they understand the process of interacting with the phishing emails that deceive them. As is typical with other interpretive studies in IS (Orlikowski & Baroudi, 1991; Rowlands, 2005; Walsham, 1995), this study aims to produce an understanding of the context in which individuals interact with phishing emails and the process by which the phishing emails influence them within that context. An interpretive approach enables us to understand the process of becoming a phishing victim from the perspectives of victims of such emails. Further, because interpretive research is also built on events that have already occurred (e.g., Isabella, 1990; Levina & Vaast, 2008), in this study, we utilize the grounded theory method, which is an interpretive research approach.

2.4.1 Methodology

To analyze and interpret the interview data, we used grounded theory techniques, which have been effectively used in recent IS research (Hekkala & Urquhart, 2013; Levina & Vaast, 2008; Vannoy & Salam, 2010). The techniques of grounded theory are suitable for capturing individuals' interpretive

experiences (Orlikowski, 1993; Rowlands, 2005). Grounded theorizing is also suitable when a research is explanatory, contextual, and process oriented (Rowlands, 2005). It enables researchers to focus on the context, process, and interpretations of key players — elements that are often omitted in studies that rely on variance models (Orlikowski, 1993). Instead of force-fitting data to a priori theory and hypotheses, an interpretive grounded theory study will derive theory from the data that is consistent with empirical observations (Eisenhardt, 1989). Further, to generalize the findings from this study, we compare them with relevant extant literature on phishing and information security. Comparisons not only show the relevance in terms of similarities and differences between our findings and those of extant research, but they also clarify the contributions of our study.

2.4.1.1 Data Collection

Our research is based on in-depth interviews with 17 subjects. The subjects, consisting of nine males and eight females, are actual victims of threatening phishing emails. The interviews took place in Finland and in Cameroon between January 2013 and March 2014. In Finland, subjects were identified and interviewed in three cities; in Cameroon, they were identified and interviewed in three provinces. Table 2 (in appendix 2) details the subjects and their backgrounds. We conducted some of the interviews in private offices and others in subjects' homes. The task of identifying phishing victims for this study was partly random and included asking random individuals in social gatherings, public places (e.g., cybercafés and restaurants), and places of work (offices). Additionally, the first author also asked his acquaintances to help in spreading the message that a researcher was seeking victims of phishing. Further, the task of identifying subjects partly involved a snowball approach (Atkinson & Flint, 2004). Through this approach, some of the subjects nominated others who have also been victims of phishing emails. Four of the 17 subjects were based on the snowball approach.

During the search for phishing victims, the field researcher always described examples of phishing emails. This approach enabled a unique opportunity to gather data directly from actual victims of phishing. The in-depth interviews were semi-structured with open-ended questions and the subjects gave permission to be audio-recorded. All the interviews were done in face-to-face communication and each interview typically lasted for about 45 to 60 minutes. The interviews started with general questions about Internet and email usage, such as how long subjects have been using the Internet and email as well as their reasons for using these technologies and their general knowledge of security on the Internet. In addition, the questions were also specific; for example, subjects were asked to describe the phishing emails that deceived them, their previous experiences with phishing emails, and anything they could remember about the phishing email and their reasons for following the instructions. The in-depth format also allowed considerable probing. Further, participation in the interviews was voluntary, and no rewards were offered to the subjects. However, subjects were promised strict confidentiality.

Some subjects indicated that they were motivated to participate because they felt the study might help prevent others from becoming phishing victims.

2.4.1.2 Analysis

Following the descriptions of how to generate grounded theory set out by (Glaser, 1978), we analyzed the data using open, selective, and theoretical coding. Glaser described the open coding process as "running the data open" (Glaser, 1978 p.56). We used open coding to analyze the text at the sentence level. The analysis involved highlighting descriptive concepts relevant to this study. Open coding was also comparative, as we constantly compared and contrasted the open codes for similarities and differences (Myers, 2013). Following open coding, selective coding was used to condense the open codes at an analytical level (Urquhart, 2013). This process again involved constantly comparing the descriptive codes identified during open coding and condensing them. Theoretical coding was the final coding phase, and it involved establishing the relationships among the categories identified at the selective coding stage, and this resulted in a core category. Exemplar codes are shown in Table 3.

Further, using an inductive approach means the grounded theorizing process was data driven, and we did not attempt to fit the data into any preexisting coding frames or our own analytic preconceptions (Braun & Clarke, 2006). The identified and analyzed codes represent the content of our interview data. Our initial research question prior to the interviews was broadly phrased: *Why do people comply with phishing emails?* However, the emerging evidence from the interviews pointed to the fact that people's attributes and online behaviors had different effects on their reasons for becoming victims. Thus, we revised the research question to: *How do differences in people's Internet behaviors and experiences affect their reasons for complying with phishing emails?* Therefore, the identified codes are based on this latter research question. The essence of a codes' saliency was in terms of whether it captured our overall research question. Both authors were involved in the data analysis. While the first author was primarily responsible for the data analysis, the second author provided feedback on the process, based on the raw interview data.

2.4.2 Findings

The five headings in this finding section depict how subjects' different online behaviors, personal attributes (e.g., Internet experiences), and changes in their diverse personal situations or relationships all interacted to affect how they made sense of the phishing emails that deceived them.

2.4.2.1 Everyday Uses of Email

All subjects stated that they have at least two personal email accounts: one for regular use (i.e., the personal email account) and another for spam emails and/or other online activities, for example, gaming, dating, or Facebook. However, subjects viewed the email accounts they used regularly as their most

important email account. For all the subjects, their years of using the Internet coincide with the years they created their first email accounts; the first email account was created in the late 1990s and the latest in 2010.

> *I first started using the email account in 2009. I opened the email account when I started using the Internet. Back then, having an email account was trendy; everyone was using email. So, I also decided to open an email account. However, I was not used to it so I think I am now using my third email account. The earlier ones have been closed. I decided to have an email account in order to easily and quickly connect and communicate with people and with my friends and family in distant places (Subject 16).*

Through regular use, their email accounts became important for their personal affairs, private transactions, and communications. Thus, when a seemingly genuine email, for example, threatened the closure of such email accounts, the subjects took the message seriously:

> *I am nothing without my email account. My Yahoo account is private; I use it for my personal affairs. Acting to protect my account helps to secure my financial transactions. I do several financial transactions through my email account (Subject 7).*

Their email accounts were not always so important; however, they have become important in their daily lives and as part of their daily routines. The accounts are used for socializing, interacting, and work.

> *My private email account is like my phone. Through it, I can be reached at all times. If anything is happening that concerns me, I will be aware immediately. I also use it for work; it's quick when I can't get up from my desk. I can socialize through emailing, while I am working (Subject 3).*

Further, one subject (Subject 8) described how he often multi-tasks while online by performing several different activities at the same time. Subject 8 noted that multi-tasking might have affected his concentration when he received a phishing email about a purchase from Amazon in a personal email account. Subject 8 regularly received spam emails through this email account. However, he would occasionally receive important emails through the email account. The subject had recently made a purchase on Amazon and was expecting the delivery:

> *I went into one of my email accounts, and this is only for spam. However, I sometimes receive some important emails in them. When I checked it, I noticed an email about one of my purchases. I think the problem with me is that I can also click on a link because when I am multi-tasking, I am distracted. For this email, I was in a really relaxed state, and, of course, it was about a problem with one of my orders.*

But to sum it up again, I think that the topic of the phishing email was relevant to me. I was interested about the topic, and the topic concerned me because I had orders. In addition, the phishing email was well written. It was a typical email. And I think lots of people like me order stuff on the Internet and maybe click those links because it is relevant to them (Subject 8).

In summary, the subjects initially created email accounts because it was trendy or for ad hoc communications. Over the years, however, they have become indispensable in the subjects' lives, for example, enabling subjects to conduct online purchases and receive updates about such purchases.

2.4.2.2 Encounters with Security

Some subjects' (e.g., Subjects 1, 3, 4, 5, 7, 9, 12, 13, and 17) decisions to comply with phishing emails were influenced by their knowledge of online security. In general, the subjects considered themselves non-expert Internet users who primarily use the Internet for emailing, browsing, and chatting. Their knowledge about security was mostly from acquaintances and the news media:

My decision was influenced by my knowledge at the time about security and privacy on the Internet. My friend told us that his account was hacked, and he started receiving sexually explicit messages and pictures. That is an embarrassing thing to happen to someone. So, of course, I was concerned that something embarrassing might happen to me. Always best to prevent such an occurrence if you can (Subject 13).

Their basic security knowledge notwithstanding, the subjects generally thought that no one would want to hack into their email accounts or steal their identities. They viewed themselves as ordinary Internet users doing ordinary things online. Yet, the threats in the phishing emails made the subjects with some knowledge or awareness about security threats fearful of losing their email accounts. One subject had ignored the phishing email. However, when a few days later she received a reminder, she felt pressured. She also saw the reminder as suggesting that the email should be taken seriously:

When I got this email that said my account will be deactivated, and that I must act by a deadline, I first ignored it. I knew there were dangers in having an email account and using the Internet. However, I didn't know that I was personally vulnerable to those risks. Yet, I also didn't want to lose my account, so as the deadline approached and the message was still sent to me again as a reminder, I felt pressured and fearful that I might lose my account. I filled in the form and gave my username, password, secret question. I share little gossips here and there; work gossip with colleagues about our bosses. Something bad happens to my account, someone accesses it and our bosses discover it, I will be so ashamed. And maybe I can lose my job.

Or what will my other colleagues be thinking of me? That it's my fault? No, I had to do something (Subject 3).

When subjects received these phishing emails, they thought it came from their account service providers (e.g., Yahoo or Gmail). Additionally, they had received similar emails before, for example, requesting that they update their passwords. When some subjects started complying with the phishing email, by submitting their usernames and passwords, these were visible. In their prior encounters, however, they were not. Despite having doubts, the subjects followed through with the request:

I received this mail that was titled, "urgent: security account update," and the message stated that if I don't update my account with certain information: my name, my date of birth, and my account will be deactivated. I believed that the email was from Yahoo account management. So, I decided to respect the request to update my information and clicked on the link. But when I was inputting my password it was visible on the monitor. Usually it is supposed to be invisible. So, I had a hunch that it could be hackers, but I just went ahead and filled in the form. That same day, my manager and one other colleague received the same email, and I advised them to go ahead and follow the requests. The next day, however, I could not access my account. It was not easy but I used an alternate email address to regain control over my account. I complied because I thought it came from Yahoo; it had all the logos. And Yahoo used to send such messages. I remember that, in 2005, I received such a message that we should upgrade, and it wasn't a problem. But when it got to the password section, it wasn't visible. When I saw that my password was visible, I asked myself is this really from Yahoo? I had doubts but I continued (Subject 17).

Even though subjects also indicated that they often delete spam emails received in their personal email accounts because they were not relevant, they regarded a direct threat against a personal email account differently.

I would regularly delete uninteresting spam emails. However, the content of the mail that deceived me was very persuasive. If the message is just an attempt to access my account, it's not appealing, but if they say my account has already been accessed, then I am very worried. My account is very valuable to me. It was authentic to me because it was signed by Yahoo, which is my email service provider (Subject 4).

In summary, the prior security encounters that some subjects had experienced made some suspicious and others fearful of the phishing emails that deceived them.

2.4.2.3 Information Security and Privacy Concerns

Subjects also complied with phishing emails to protect their financial and personal transactions. These concerns made some subjects interpret the phishing emails as threats against their need to keep certain information and messages private:

> *Confidentiality of my account is very important to me. There are certain things one has to keep from others. If I was not very sure of the message or where it's from I would not have bothered to click on the link (Subject 7).*

Given the volume and nature of the communications, contacts, information, transactions, chats, and messages in their personal email accounts, some subjects also feared a possibility that an exposure would result in ridicule, embarrassment, or damaged relationships. Some subjects even worried about being blackmailed as a result. Because subjects wanted to maintain harmonious relationships, some subjects felt the need to comply with the phishing emails:

> *The phishing email stated that my account has been breached. In my email account, I have different kinds of relationships with my friends. We discuss different kinds of private chats. It can be embarrassing if the things my friends share with me and I with them were exposed to everyone. What do I tell them? I also have my own secrets in those conversations. Given that it says hackers breached my email account, I worried they can further blackmail or threaten me. I feared that they will threaten to expose everything about me and bring shame on me and my friends. With these thoughts going through my head, I knew I had to act (Subject 5).*

Another fear was that losing a personal email account might cause unnecessary problems. Subject 11, for example, believes it is responsible behavior to take a seemingly legitimate phishing email seriously, suggesting a breach of privacy must be taken seriously.

> *The message said my account has been breached, that there was unusual activity in my account. I first thought that maybe somebody out there is watching me and my email account without my permission. Everybody has a kind of confidentiality. When an account is breached, it exposes those things that you are keeping secret, so I definitely don't want someone to see something that I am keeping confidential. And it may affect all my correspondences and friends. So, I think when I received such a message and it looked legitimate, I had to react to it for confidentiality reasons (Subject 11).*

One subject reported that he was concerned about the security of a purchase he made from Amazon. His goal in clicking on the phishing message was to find out what was wrong. The message indicated that there was a security problem with the tracking of his Amazon purchase:

The email suggested that a purchase I had made had some problems – a security breach affecting its tracking. I do most of my purchases online, so I can't keep track or am not very interested to keep track of them, so I thought to myself, let's check it out. I accessed the phishing message, and I clicked on the link. I actually clicked the link. I am using Firefox at home, and when I clicked the link, my Firefox browser, which was of course updated, didn't go to the webpage, and it actually warned me that it was suspicious link and then I stopped. So, Firefox, the software saved me, or I don't know what would have happened if I had gone to the webpage. I thought about it for a while that how can I be so stupid that I clicked on the link (Subject 8).

In summary, the subjects who had security concerns imagined several worse-case scenarios that were likely to happen because of a security breach of their email accounts. These imaginings as much as the security concerns emphasized in the phishing emails caused them to click on the phishing emails.

2.4.2.4 Encounters with Phishing Emails

When subjects encountered the phishing emails that deceived them, most thought the sender's intention was good; that is, to secure their email accounts and consequently, their personal information and privacy:

The phishing message said my account has been breached. I feel concerned about the email because I wouldn't want my mail to be hacked or someone to illegally access my mails. I rely on my email account a lot: for personal transactions, purchases, family, and friends. I had to click on the phishing email after reading it. The email said my account has been breached and that I must act immediately. That way, my account can be protected before the hackers completely takeover it (Subject 13).

The phishing emails were also interpreted as assistance to ensure their email accounts and their content remain secured. This message resonated with subjects who wanted to control how information about them is communicated and to whom:

The message stated that in the next 24 hours my account will be closed. When I read the message, I felt that the intention is good to secure my account. I don't want my account to be deactivated in the next 24 hours. Some of the mails and photos in my email account are private and should not be accessed. In addition, I also have some private stuff that I don't want everyone to hear about. My image is important (Subject 14).

Despite their prior experiences with similar requests, the attributes that make phishing emails appear authentic and legitimate also make it hard for subjects to distinguish phishing emails from legitimate emails. Thus, their

concerns for their information privacy and limited experience lead them to the wrong decisions:

> *You know it is very difficult to determine that its fake because, at the end of the message, it said it is coming from Yahoo admin. It also stated that if I don't click on the link, it will allow other people to access my account. I don't want other people seeing my online activities (Subject 7).*

> *After reading the phishing message, I became concerned about my privacy and about an exposure of some of my online behaviors. Everything really looked authentic, so I had every reason to act as I did (Subject 12).*

2.4.2.5 Complying to Protect Email Accounts

The fact that the subjects received these phishing emails in the email accounts they consider to be important influenced their decisions to comply. Based on their existing security knowledge, the subjects did not want others to have access to their email to compromise their privacy:

> *The phishing message was about an urgent security update regarding my user account. The goal was to secure my account, and the message emphasized that if I don't act to secure my account, people can get into my account. By acting to secure my account, I was blocking these bad people and keeping my account secured. It is important for me that my email account is secured because, first of all, my email account is very confidential to me. I have both confidential information and mails, photos, and many things that concern only me, so I want them to be very secured (Subject 9).*

In addition, they felt that they could not afford to do nothing and have their accounts deactivated:

> *It was an account deactivation notice phishing email. It very precisely stated that some people tried to log into my account and if I do not change my password, my email account will be closed in the next 24 hours. So, I do not want to lose the information that I have in my account and I don't want it to somehow be accessible to other people. As a result, I clicked. My email is private, and if it is deactivated, so many vital information will be lost (Subject 2).*

One subject complied because the email account under the threat of deactivation was an important business account. As manager of a shop, she used that account to communicate the businesses' financial performance to its owners. Ensuring the account was protected and functional was therefore a priority:

When I received an email that said my account will be deactivated within 24 hours unless I update some of my personal information, I felt compelled to act because I didn't want my account to be deactivated. At that time, I was managing a shop, and although I sometimes communicated with Yahoo Messenger, I more often communicated through my personal email account. I sent emails to the owners of the shop to update them about the situation of the shop. I also sent monthly financial statements of that shop to the owners through my Yahoo email account. Therefore, I had lots of records about that shop in that Yahoo email account. I was complying with the phishing request and thinking I don't need to lose this account. Since that phishing incident, I now have two personal email accounts, and I valued the one that was hacked more because I used it for communicating the financial transactions and the financial situation of the shop. It was also the email account I have been using since the year 2000. As a result, it had many contacts and information in it that I did not want to lose (Subject 1).

2.5 Discussion

We make sense of these findings by explaining why diverse individuals with different backgrounds and experiences comply with threatening phishing emails. In doing so, we propose a stage theory that comprises two categories of people in two stages (Stages 1 and 2). By categorizing phishing victims this way and developing a stage theory to explain their reasons for complying with phishing emails, this work extends existing security research by presenting an empirical study on the phishing behaviors of diverse individuals outside an organizational context. Extant phishing research has identified a small set of fixed/static predictors or explanatory factors as reasons people comply with phishing emails. These factors are assumed to remain the same across individuals despite the differences stemming from their individual attributes and online behaviors.

We argue that individuals' reasons for using email and the Internet change as their online behaviors, security experiences, and personal circumstances change. Consequently, understanding where individuals reside at particular points during their online experiences means anti-phishing measures can be developed and tailored to their immediate needs. Thus, we argue that the actual act of complying (e.g., clicking on a phishing link or attachment) remains the same across individuals; however, the differences emerging from individuals' years of Internet experiences, security experience, and online behaviors affect how individuals process phishing emails differently. We addressed this problem by studying the following research question: *How do differences in people's Internet behaviors affect their reasons for complying with phishing emails?*

2.5.1 Toward a Stage Theory of Phishing Victims

As stated, our proposed stage theory categorizes individuals susceptible to phishing as residing in two stages. Table 1 describes the components of our stage theory. A stage is defined in terms of the process attributes of the residents of that stage (i.e., user attributes and user behaviors). From these process attributes emerge reasons that highlight the differences between residents (i.e., phishing victims) of each stage. Each process attribute highlights differences between Stages 1 and 2 and shows that Stage 1 and 2 residents complied for different reasons. The stages and change elements indicate interdependent relationships highlighting how, by themselves, the phishing emails are not sufficiently persuasive to deceive individuals' into complying with phishers' requests.

The process model (Figure 1) shows the processes involved in complying with a phishing email and how Stages 1 and 2 residents differ from how they processed the phishing emails that deceived them. The dispositional attributes that individuals in the different stages possess are not fixed but are temporal. For example, through further exposure and training or education, a Stage 2 resident can progress to a stage where residents can identify a security threat and know how to manage that threat.

Further, the different attributes that make up the different processes help us understand what is happening to individuals who are at a particular stage. In addition, each stage and process has change elements that are process-specific attributes that explain how individuals arrived at their respective stages. The four process attributes (the nature of email and Internet use, prior encounters with security, information security and privacy concerns, and encounters with phishing emails) are used to explain why some individuals reside in Stage 1 and others in Stage 2. According to our categorization, the residents in Stage 1 comprise Subjects 2, 3, 12, 14, and 16, whereas the Stage 2 residents comprise Subjects 1, 4, 5, 6, 7, 8, 9, 10, 11, 13, 15, and 17.

TABLE 1 Table of stage theory

Stages	**User Attributes**	**Time**	**User Behaviors**
Stage 1 elements: -user attributes -user behaviors	- Perfunctory/ad hoc - Irregular or infrequent Internet users: "Followers" using email and Internet because everyone is using it	1	Nature of usage behaviors: Nature of uses (personal) General Internet use (e.g., browsing the news) Email use Ad hoc/perfunctory or mundane activities
Change elements	Process of change describes how people arrived at a particular stage, that is, the reasons people reside at particular stages. The reasons are based on: Change in nature of email and Internet use behavior stemming from new online behaviors (e.g., creating, storing, and sharing information and transactions) Exposure, encounters, or interaction with security-related issues online		
Stage 1 change elements	*Security knowledge* - Identifying security problem - Do not understand security problem - Uncertainty about security solution: cannot independently identify a solution *Perception of phishing email:* - Phishing email is unwanted interference, problem to online behaviors - Phishing email provides solution to the problem		
Stage 2 elements: -User attributes -User behaviors	- Nature of use: personal and business - Have personal information and security concerns (e.g., exposure, blackmail)	2	- Frequent email and Internet users - Dependence on technology and its benefits for banking, gossip, business transactions, creating, storing, and updating files, photos, and private transactions. - Using multiple online services, creating, storing, and sharing information and transactions.
Stage 2 change elements	*Security knowledge:* - Identifying security problem - Understands security problem - Uncertainty about security solution (what to do) *Perception of phishing email:* - "Perception of phishing email" from stage 1 - Threatening personal information and privacy - Having doubts about the solution		
Outcome behavior	Comply with threatening phishing email		

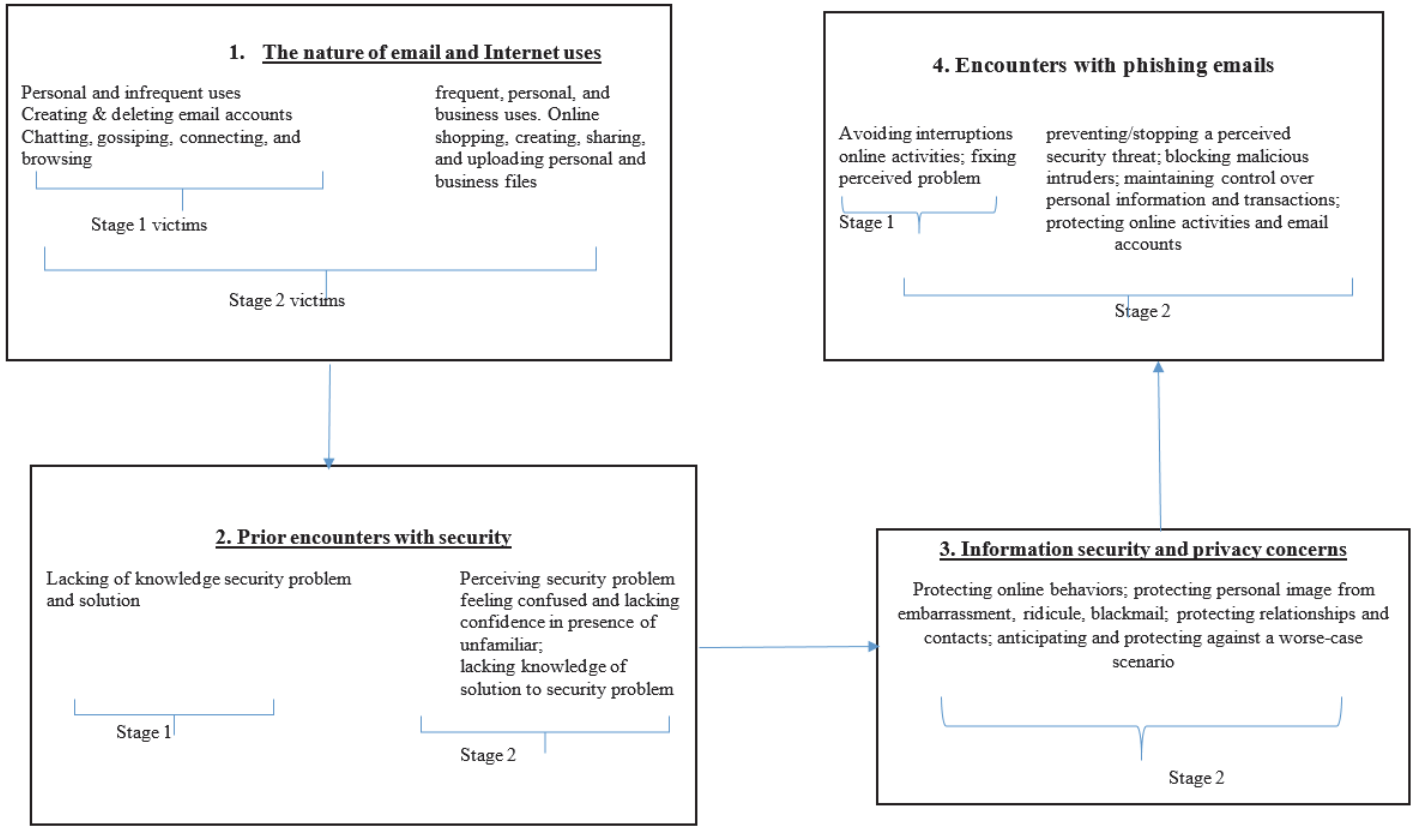

FIGURE 1 A process of complying with threatening phishing emails

Note: numbers in the boxes refer to the processes as outlined in the discussion section

2.5.1.1 Process 1: Nature of Email and Internet Use

Stage 1 victims use email and the Internet for several reasons, for example, because it is trendy, for general browsing, and for communicating with family and friends. Some Stage 1 victims use email and the Internet for ad hoc or perfunctory activities (e.g., "everyone was using email" (Subject 16). Others, however, can be regarded as using the Internet and email for personal chats with relatives and friends. Although the personal use behavior is similar between Stage 1 and 2 victims, Stage 2 victims can be described as more sophisticated users. The nature of online use for Stage 2 victims is more frequent, and the personal/business use behaviors include creating, storing, and sharing personal photos, information, and secrets. Stage 1 victims wanted the perceived problems in the phishing emails addressed so that they could continue with their activities. Stage 2 victims, moreover, became concerned about their online behaviors (personal/business transactions), primary email accounts, and online contacts and relationships. Whereas the nature of use for all Stage 2 victims has evolved from rudimentary conversations to more personal and business transactions, the same cannot be said for all Stage 1 victims.

This finding addresses the problem of general Internet usage in the phishing literature. Past phishing research suggests that, because frequent Internet users are more familiar and exposed to emails, they are more likely to detect phishing emails (Harrison, 2016). Our finding on the nature of the Internet and email use suggests that it only represents the first process of becoming a phishing victim. Individuals' reasons for not ignoring or for taking the phishing message seriously are different for Stage 1 and Stage 2 victims. Whereas Stage 1 and 2 victims were affected by a perception of legitimacy and authenticity, Stage 2 victims were also affected by concerns for their online behaviors and accounts.

Furthermore, because changes in their reasons for complying were influenced by their more personal use of email and the Internet, subjects had an expectation of control over the access to their respective email accounts. Thus, the changes in email and Internet behaviors from ad hoc to regular and from mundane to personal (private) and business activities were the Stages 1 and 2 subjects' main reasons for seriously considering the phishing emails at this stage of the phishing deception process.

As is typical with continuum models, past phishing research has found a direct relationship between general Internet use and phishing compliance; however, our stage theorizing suggests that general Internet use explains why phishing victims did not ignore the phishing messages in the first place. Our theorizing also shows that differences in individuals' reasons for using the Internet or email affect how they formed their impressions of the phishing email requests.

2.5.1.2 Process 2: Prior Encounters with Security

This stage addresses the role that subjects' prior encounters with security had on how they understood the threats in the phishing emails that deceived them.

Whereas the Stage 1 victims cannot identify a security threat and a solution to the threat, Stage 2 residents can identify a security threat, but not a solution to the threat. Prior to encountering the phishing emails that deceived them, the residents of Stages 1 and 2 had encountered security threats during their online use behaviors.

Although Stage 1 residents can be aware of online security threats, they can neither recognize nor solve a security problem. Upon encountering a phishing threat, and perceiving the email as authentic, their primary concern is not about the consequences of compliance, noncompliance, and fear of consequences (negative or positive); rather, it is about doing what they think must be done to fix the problem, thereby getting the problem out of the way. Consequently, Stage 1 residents will disproportionately focus on the phishing attributes. This finding on Stage 1 residents is similar to several past phishing studies in which researchers have reported that victims are more likely to focus on elements of the phishing emails that reduce elaboration and systematic processing, for example, email title and source and urgency cues (Vishwanath et al., 2011).

By contrast, the finding on Stage 2 residents suggests a more nuanced role for prior security knowledge. Concerning Stage 2 residents, we suggest that confusion resulting from residents' prior experiences with conflicting security messages gives rise to a lack of confidence, which influences subjects' decisions. Because prior phishing knowledge is assumed to affect elaboration, researchers have found that individuals are more likely to detect deceptive cues in phishing emails (Wang et al., 2012). Drawing from cognitive and consumer psychology (Cowan, 1986), security researchers have theorized that deceptive cues emphasizing the urgency of response interrupt rational decision-making processes (Vishwanath et al., 2011). However, prior phishing knowledge was found to reduce the risk of complying by enabling users to engage in rational decision making (Wang et al., 2012). Such individuals have high computer self-efficacy and confidence in handling online security threats, making them less likely to comply (Wang et al., 2012; Wright & Marett, 2010). Despite their prior security experiences, Stage 2 subjects were not confident in handling phishing emails. Their prior security knowledge that comes from the mass media, experience with spam emails and/or phishing emails, and from interacting with acquaintances was not sufficient to detect the phishing. Thus, although Stage 2 subjects do not regard phishing emails promising wealth as persuasive, consistent with prior findings on inexperienced Internet users (Dodge, Carver, & Ferguson, 2007), subjects acknowledged being prone to mistakes when the phishing email has an authentic look and feel.

Stage 2 subjects' prior security encounters motivated them to take the phishing security threats seriously; however, they could not manage the phishing emails with which they were unfamiliar (Downs et al., 2006). Confusion ensued because the right decision oscillates between clicking on some links and not clicking on others. The lack of confidence was the result of the observable discrepancies with what they are used to handling. Accordingly,

we suggest that prior security experience makes frequent Internet users with limited security experiences confused when the phishing emails are authentic looking. Because the source of the confusion is their limited experience, they become less confident and adopt a mistaken protective behavioral stance.

2.5.1.3 Process 3: Information Security and Privacy Concerns

Because the Stage 1 residents can neither understand a security problem nor identify the right security solution, this finding is based on Stage 2 residents. This finding suggests that security threats in phishing emails give rise to personal information security and privacy concerns, as individuals fear negative consequences of a breach on their information security and privacy. Prior phishing research has not addressed this important issue. Rather, the primary focus has been on the user attributes (Wright & Marett, 2010) and persuasive phishing factors (Wang et al., 2012; Harrison et al., 2016) that increase susceptibility to phishing. (Workman, 2008) reported that users comply with phishing emails because they are careless about their security. Admittedly, subjects processed information security and privacy concerns because the phishing emails emphasized security problems. In addition, security researchers have reported that the presence of a threat element in a message makes the message more persuasive (Das, de Wit, & Stroebe, 2003). Despite their security and privacy concerns, however, subjects focus on the personal ramifications of becoming a phishing victim, clouding their judgment. We suggest that subjects' security and privacy concerns involve a fear of surveillance and/or a violation of privacy. Moreover, we suggest that they desire to protect their email accounts and the confidentiality of their contacts and communications. Thus, their concerns were the combination of the phishing emails emphasizing security problems, the subjects' frequent and varying uses of email, their prior encounters with security and other phishing attempts, and their beliefs that a personal email account is a private space.

Further, their thoughts also veered toward a fear that an intrusion could lead to blackmail and damaged relationships. In creating, sharing, and storing personal information, transactions, and contacts in their respective email accounts, the subjects assumed they had control over access to the accounts. However, despite their fears (e.g., blackmail) and security concerns, subjects were never sure that their privacies had not been violated; in other words, they had doubts. Because these thoughts disturbed their equanimity, they feared the possibility of an intrusion to their privacy. Thus, encounters with threatening phishing emails create a belief of an information security and privacy breach. Threatening phishing emails motivate individuals to become immersed in the emails as they consider the meaning within a larger personal context.

Overall, we report on the role that information security and privacy play in being deceived by threatening phishing emails. We report that, when individuals make decisions about a threatening phishing email, they comply because the possibility (fueled by their prior security encounters, frequent use of email, and their beliefs) that the phishing message may be true overrides the

other possibility (fueled by their doubts, confusion, prior security encounters, and frequent use of email) that the phishing message is a phishing attempt.

2.5.1.4 Encounters with Phishing Emails

Stage 2 subjects' perception of a threat to their personal email and information security motivated them to want to block any (potential) malicious intruders from accessing their email accounts. Stage 1 subjects' perception of an interruption of their online activities motivated them to comply with the threatening phishing emails. This finding contributes to how individuals' reasons for complying are formed when they encounter threatening phishing emails. It explains how individuals' prior security encounters affect how they view the elements of phishing emails that emphasize legitimacy, authenticity, relevance, and threats. While specifically focusing on the reasons for subjects' behaviors, our finding contributes to prior research on why people comply with phishing emails (Wright et al., 2014).

Based on research in persuasion, prior phishing research has identified scarcity, social proof, reciprocity, consistency, authority, and trustworthiness (Wright et al., 2014) as the influence techniques or cues used by phishers to make people comply with phishing emails. Identifying which techniques influence individuals' thinking processes no doubt contributes an important explanation regarding why people comply with phishing emails. However, the researchers' focus on adopting these influence techniques was to determine which elements of phishing emails people focus on when they encounter a phishing email.

Similarly, research on home users' security behaviors seek to understand why this group of users became victims of diverse security attacks. The findings suggest that when users perceive a threat (threat susceptibility) and the severity of its negative consequences (perceived severity), they become motivated to avoid the threat if they believe that the safeguarding measure is effective, inexpensive, and they have high computer self-efficacy (Liang & Xue, 2010).

In past studies on phishing behaviors and general home user behaviors, researchers did not account for the changes affecting users' reasons for thinking and acting as they did. First, we suggest a retrospective thinking process whereby a phishing email activates individuals' information privacy concerns. Next, the thinking leads individuals to extract or rely on the knowledge from their prior security encounters to make sense of what is occurring. Even when subjects had doubts and/or suspicions about the source of the email based on their prior encounters with security, the elements of the phishing email that project legitimacy, helpfulness, and credibility (e.g., the source being the management of Yahoo) combined with their personal information and security concerns persuaded them to take the phishing email seriously.

The resulting preemptive thinking is influenced by their prior security encounters. On one hand, these prior encounters focused individuals' thinking processes on fears that malicious entities have access (or may have access) to knowledge or relevant data about them; in addition, they had fears that they may lose/have lost control over their privacy. On the other, because of subjects'

prior security encounters, their thinking was also confused. While phishing emails elicit information privacy concerns, they also elicit confusion for two reasons: (1) subjects are not comfortable with how they are supposed to resubmit their personal information (e.g., on a form that makes the password visible) and (2) because subjects know they are not knowledgeable enough, they also lack the confidence to ignore the phishing email. Consequently, they were driven to click on the phishing emails by their intention to block malicious entities. Whereas such intentions result in protective behavior in studies conducted in the home context (Anderson & Agarwal, 2010), they resulted in security breaches in a phishing context. This suggests that to translate a protection motivated action/behavior to result in actual protection, the individual must not only have security knowledge and self-efficacy, as suggested in past research on phishing and home users, but more importantly, the individual must also have specific knowledge or be advised about how to act in that context.

In summary, our findings suggest that the subjects in prior phishing research can be categorized as either Stage 1 or Stage 2 residents. However, this categorization is not definitive and there is likely to be a third or even fourth categorization of phishing victims. Importantly, the reason for this categorization is the differences in victims' online behaviors and experiences, which affect how they comply with phishing emails. For example, we find that Stage 1 residents can neither recognize a security problem nor identify and utilize a security solution. In contrast, Stage 2 residents can recognize a security problem; however, they cannot extrapolate to understand and utilize the correct security solution. This means anti-phishing recommendations should first identify where victims reside before rolling out the recommendations to ensure they are effective and targeted at the right persons. By extrapolating to derive two categories of phishing victims, we can make anti-phishing recommendations that are tailored to each specific category of Internet users.

2.5.2 Implications for Practice

Past phishing studies have advanced several recommendations aimed at reducing the likelihood that people will continue to become phishing victims. Among the recommendations, security education, awareness, and training are often cited as enabling people to detect and avoid the persuasion techniques used by phishers (Wright et al., 2014; Wright & Marett, 2010; Sheng et al., 2010; Kumaraguru et al., 2009). Overall, past studies suggest that anti-phishing training should ensure individuals can distinguish between legitimate and phishing emails. In particular, an embedded training approach (Kumaraguru et al., 2007) emphasizes that users be educated about the risks of identity theft and financial loss by (1) teaching users that phishers are out to steal their information and (2) training users never to click on links within emails, to always type the real website address in a browser, to be suspicious of websites, and to call customer service (p. 2). The basis of these recommendations is that

people click on phishing links because they perceive the phishing emails to be associated with a legitimate brand (Ormond & Warkentin, 2015).

Based on our findings and our proposed stage theory, we make the following recommendations for practice.

Adopting lessons from a stage-based approach

The findings from this research highlight how people's varying levels of experiences (individual attributes) and online behaviors should affect the design and implementation of anti-phishing recommendations. In the extant phishing research, however, the basis of the practical recommendations neither considers nor explains the matching of practical phishing advice to the specific needs of Internet users. In other words, past researchers do not consider that recommendations might be more effective when tailored to people based on their knowledge, skills, and Internet experiences. Thus, the current strategy in the phishing literature is based on a "one-size-fits all" approach.

We have shown that people at Stage 1 comply for reasons that are different from people at Stage 2. This is because peoples' residence at particular stages at different points in time directly affects their online security knowledge and general online use behaviors. Residing at a particular stage has a bearing on a person's security knowledge, self-efficacy, and experiences. Consequently, we recommend that anti-phishing programs adopt a stage-based approach, considering individuals' reasons for residing at each stage. Thus, in developing anti-phishing recommendations, security experts ascertain the needs of the targeted user groups. For making practical recommendations that are efficient and effective, we propose separating people into at least two distinct stages.

The first step should include assessing and acquiescing the needs of individuals based on their resident stages. While this approach will serve to avert mismatching recommendations, it will also ensure that recommendations are tailored to meet the specific attributes and behaviors of the people residing in each of the two stages. Second, security experts should specify the precise behaviors that need to be changed. The key behavior that needs to be changed is clicking on phishing attachments and links. Based on their specific user attributes and online behaviors, we recommend rolling out recommendations for Stage 1 individuals that will discourage them from clicking on links. The messages should aim at developing a general awareness about phishing and cybersecurity threats. This is a basic approach to security. However, it is necessary for Stage1 individuals because they neither understand the security problem nor its solution.

Anti-phishing programs for Stage 1 individuals should aim to create an awareness about online risks, such as phishing and Internet scams. They should also aim to change peoples' perceptions, for example, that it is not okay to click on links simply because they appear to be personally relevant and that anyone can become a phishing victim. Emphasis should also be on the types of deception methods being used by phishers. While the message is basic, the specific security problem (i.e., phishing) is emphasized to enable individuals to link the problem to the solution (awareness about phishing). For example, Stage

1 individuals can be made aware that changes to their email personal information cannot be done through a link. Therefore, companies are unlikely to request that they do such changes through a link. Although it is typical to find such messages in anti-phishing newsletters, they are not targeted at a particular user and are designed to benefit all Internet users. Mismatched interventions probably contribute to why anti-phishing techniques are not always working or why their effectiveness is often for a short-lived period (Kumaraguru et al., 2010).

By contrast, for Stage 2, the reasons for using email and the Internet have evolved, and these people are more familiar with online security threats. Thus, the generic messages that seem appropriate for the people in Stage 1 become useless. Such messages add little value because the attributes of Stage 2 individuals suggest that, although they lack specific security knowledge to protect themselves, they are already security aware users. Stage 2 people can understand the security problem but not extrapolate and identify the right solution.

Thus, they become confused and lack confidence in what they should do when faced with a threatening phishing email. Because they rely more on the phishing messages' relevancy and legitimacy attributes, we suggest that anti-phishing messages should focus one or two specific messages that people in Stage 2 can satisfactorily perform. These messages should also be used consistently to avoid confusing users, for example, asking them to focus on a specific portion of the phishing message, such as the source or URL. Given that they are more experienced online, people at Stage 2 can be encouraged to systematically verify the authenticity of a link before deciding to click on it. The literature on phishing overwhelmingly advises that people do not click on suspicious links or attachments. Although advising people to focus on specific portions of a phishing message is often mentioned in the literature on phishing (e.g., Harrison et al., 2016), researchers have also noted that the advice is rarely followed (Wu, Miller, & Garfinkel, 2006). We believe this is because security experts are targeting the wrong audience. Anti-phishing messages are less likely to be effective when they are addressed to individuals belonging to the wrong stage.

Educating to build people's confidence

In general, Stage 1 and 2 individuals are motivated by their reasons for using the Internet when deciding to comply with a phishing email. Indeed, we found that, by utilizing phishing emails that emphasize threats, phishers can make Stage 1 and 2 residents comply out of fear of the security threats emphasized in the phishing emails, albeit for different reasons. For example, Stage 1 residents comply because they focus on the messages' perceived authenticity and legitimacy; however, Stage 2 residents are more likely to comply because they tend to disproportionately focus on protecting the reasons for their online behaviors (e.g., personal and business transactions).

Therefore, anti-phishing education and awareness programs should specifically make people aware that phishers are hoping they will comply out of

personal information and security concerns for their online behaviors. In particular, because of their current security knowledge, people in Stage 2 are confused and doubtful of their abilities. Past researchers have reported that increased security awareness will likely also lead users to become temporarily more suspicious (Wright & Marett, 2014). Although suspicion will likely increase the number of false positives (Kumaraguru et al., 2010), we believe suspicious users are better-off than doubtful or confused users because they are less likely to comply with phishing requests. Thus, while education and awareness will boost individuals' confidence, those who have doubts during an interaction with a suspicious email should be taught to rely on their gut instincts.

Using protection motivation and fear appeals in anti-phishing programs

Phishers use fear appeals in the form of threats requiring phishing recipients to urgently click to avert something bad from happening or to reduce the negative effects of an already bad situation (e.g., a security breach that has already occurred). In the IS security literature, fear appeals represent a popular approach to enhancing peoples' motivation to perform protective behavior (Johnston & Warkentin, 2010). Our finding indicates that the use of fear appeals in phishing emails result in mistaken protective behaviors among phishing victims. Although they can recognize a security problem, our finding suggests that Stage 2 residents become victims because they have low self-efficacy in relation to recommendations they do not understand (e.g., checking a messages' source, placing a cursor above a link, or checking the URL). Thus, recipients of phishing emails may choose to protect themselves by performing the most obvious and simple protective action recommended by phishers. For example, they may comply because they perceive the message to be legitimate and its source to be authoritative. Thus, in a phishing context, we recommend that using fear appeals to teach against clicking on phishing links should be avoided or used cautiously until new empirical evidence finds otherwise. Further, because Stage 2 individuals can become confused or doubtful, we recommend educating them to adopt a protective behavioral stance in which they do not click on emails that create confusion in their minds. They should be aware that a protective behavior can also mean that one should do nothing.

2.5.3 Limitations and Research Implications

Although this study is based on subjects with different variants of threatening phishing emails, the other type of phishing email (i.e., "you have won," "congratulations," or "help me") was not examined in this research. In addition, as previous phishing research has not studied this type of phishing email, it represents a new possibility for future research. The findings will likely further contribute to new factors or attributes of theoretical relevance to the reasons people are deceived by phishing emails. For example, given the nature of phishing emails with benefits, it is possible that people are persuaded by a combination of greed, wishful thinking, or altruism. These could be studied in

future research on phishing emails promising benefits. Future research could also rely on multiple actual victims of phishing to understand how the victims formed their interpretations of such phishing emails.

Our study is based on interviews with individuals from diverse backgrounds, with diverse and dynamic reasons for using email and the Internet and with diverse online security experiences and encounters. The individuals can be classed as home users in the IS security literature (Anderson & Agarwal, 2010; Liang & Xue, 2010). In developing a stage theory, we have shown how individual attributes and online behaviors affect compliance with phishing emails. In the extant phishing literature, however, researchers have viewed being deceived by phishing activity in terms of fixed or static phishing and user factors. However, our finding that victims reside in at least two stages based on their use behaviors and experiences indicate that the dispositional attributes that affect compliance with a phishing email are rarely static. We therefore recommend that future studies on phishing assume that peoples' reasons for complying with phishing emails are changing over time. In addition, the stages that people belong to demand continual adjustment, as they are affected by their changing personal situations, experiences, and improvements in the phishing emails.

Further, from our findings, subjects' concerns for their personal information security and privacy were driven by the nature of their online transactions. Given their diverse needs, we believe shame or a fear of shame has a temporal or fluctuating role in compliance with phishing emails based on certain aspects of some users' online behaviors. Indeed, anecdotal evidence from our interviews with subjects for this study seems to point to a role of shame or fear of shame. For example, future research can design an experimental survey that includes additional questions pertaining to when shame and the fear of shame are relevant, when they become relevant, and for whom. The finding will contribute to why people comply with phishing emails.

Finally, future research should utilize our stage-based recommendations in an intervention study. The intervention study will consider individuals' attributes and online behaviors. Researchers should consider the possibility of at least one additional stage (e.g., Stage 3). For example, it is possible that people could become victims because of overconfidence in their abilities to detect phishing emails.

2.6 Conclusion

Phishing attacks represent a major form of monetary loss and information security and privacy breaches. Previous research has examined why individual attributes (e.g., education and security experiences) and phishing attributes (e.g., urgency cues, threats, and fear) make people susceptible to phishing attacks. Moreover, past research assumes that phishing victims are motivated to comply by the same static or fixed reasons, irrespective of differences in their

individual attributes and online behaviors. However, we have argued that the act of clicking on a phishing email remains the same across different phishing victims. The reasons for complying, by contrast, are different for different phishing victims because of differences stemming from their dispositional attributes (years of Internet experience or security knowledge and varying online behaviors). Therefore, in this study, we examined how differences in people's experiential attributes (e.g., security experience) and online behaviors affect their reasons for complying with phishing emails. Our findings show how differences in process attributes lead people to comply for different reasons. We highlighted the differences between Stage 1 and 2 residents through the following processes: nature of email and Internet use (Process 1), prior encounters with security (Process 2), information security and privacy concerns (Process 3), and encounters with phishing emails (Process 4).

Further, we categorize phishing victims as residing in one of two stages. Stage 1 residents can neither recognize a security problem nor identify and utilize a security solution. In contrast, even though Stage 2 residents can recognize a security problem, they cannot extrapolate to understand and utilize the correct security solution. We reported that Stage 1 residents complied from focusing on and taking the phishing emails' claims, authenticity, and legitimacy at face value. Stage 2 residents, moreover, complied because their inadequate security knowledge makes them confused, doubtful, and lacking in confidence. Thus, Stage 2 residents adopted a mistaken protective motivated behavior regarding their information security and privacy. Based on these findings, we have recommended a tailored approach that highlights how people's varying levels of experiences (individual attributes) and online behaviors should affect the design and implementation of anti-phishing recommendations. This new approach should replace the current strategy based on a "one-size fits all" approach in the extant phishing research. We have also recommended important avenues for future research, which assume that the factors increasing compliance with phishing emails are rarely static or contained within a discrete timeframe. Instead, they are more likely to be unfolding over time as individuals' email and Internet experiences, online behaviors, and the reasons for their online behaviors change and/or adjust to new challenges embedded in future phishing emails.

3 STUDY II. HOW ONE BECOMES AN INTERNET SCAMMER: TOWARD A STAGE THEORY

3.1 Summary of Study II

Internet scams are a major form of Internet crime. Internet scammers use misrepresentation and persuasive communication in online interactions to swindle Internet users. Extant academic Internet scamming research has proposed three main reasons that individuals become Internet scammers: (1) monetary rewards, (2) disillusionment with socioeconomic and political problems (corruption, unemployment, and poverty), and (3) affordable access to the Internet. We argue, however, that many individuals who like monetary rewards are experiencing the above-mentioned problems and are enjoying affordable access to the Internet do not become scammers. Further, we note that scamming research is hindered by problems with gaining access to scammers, resulting in reliance on secondary data. This study is an interpretive study that uses the inductive approach to interview Internet scammers to address these problems by studying the following question: *How does one become an Internet scammer?*

First, our empirical findings contribute to determining why people become scammers by explaining why money is a motivator. We report that money is needed to socialize, to enjoy an extravagant lifestyle, and to become financially independent. Second, we contribute to determining how individuals become scammers by identifying three stages. Stage 1 contributes to determining pre-scamming activities and relationships that produce negative emotions that motivate individuals toward scamming. Stage 2 contributes to determining specifically why individuals become scammers through their associations, lifestyle preferences, and desires to maintain financial independence. Stage 3 explains why scammers use neutralizations, deterrence, and rely on third parties (pickups) to justify persisting as Internet scammers. We analyze these findings by relating them to theories in criminology. We report that none of the extant dispositional crime theories that explain

proclivity toward criminality (e.g., social learning theory) can adequately explain why people become scammers. We also report that, although situational crime theories (e.g., routine activities theory) were developed to explain why criminal acts occur, they cannot adequately explain why scamming occurs because they can neither explain the role of the offender nor the role of the computer-mediated environment in criminality. For practice, we propose that interventions will be more effective when they consider the locales that scammers operate from and the scammers' subjective assessments of deterrence and emphasize education and fear for scammers and would-be scammers.

3.2 Introduction

Internet scams in which scammers mislead a buyer or an investor in an online transaction are well-known threats enabled by the Internet. Internet scams have morphed from traditional face-to-face scams, which some researchers have traced back to the eighteenth century "Spanish Prisoner Scams" (Peel, 2006). The act of Internet scamming involves misleading online buyers to make advance payments for nonexistent merchandise, such as pets, coffee, romance, and insects. Internet scammers typically frame these advance payments as incidental costs (i.e., logistics costs: freights, flights, quarantines, or insurances) that are required before a buyer's merchandise can be authorized by custom officials for shipping (Salifu, 2008). However, such Internet scammers do not possess the merchandise they advertise, and they have no intention of acquiring and/or supplying it. Since scamming became an Internet phenomenon, Internet scammers have also become a global concern. In 2013 alone, the losses from Internet scamming were estimated at US$ 12.7 billion (Ultrascan, 2014). Although such scams have previously been mainly associated with certain West African countries (e.g., Nigeria, Cameroon, and Ghana), estimates suggest Internet scammers and their victims come from around the globe. The highest numbers of Internet scam complaints were from the United States, Canada, the United Kingdom, Australia, and India (IC3, 2013).

However, little empirical research has been conducted on Internet scammers and/or their activities. Even as their activities dominate the headline news, Internet scammers are not easily identifiable, and Internet scamming is conducted in secret. Moreover, few rigorously conducted empirical studies on Internet scammers have been published. Our current understanding of Internet scammers involves descriptive accounts of the scamming process (Atta-Asamoah, 2009), and anecdotal evidence from friends of scammers (Abia et al., 2010), police and bank officials (Ampratwum, 2009), and relatives of Internet scammers (Burrell, 2008). Although many researchers have attempted to study Internet scammers, we are aware of only one academic study (Burrell, 2008) that provided evidence from Internet scammers (n = 3). However, Burrell stated that the interviewed scammers had not made any money from their scamming activities. We are therefore not aware of any academic studies that have

interviewed actual Internet scammers who have financially benefited from scamming.

Thus, research on scammers remains at the exploratory stage with secondary sources. Consequently, this study adopts the following research question: *How does one become an Internet scammer*? We address this question by adopting the inductive process associated with interpretive research (Rowlands, 2005). This study is based on face-to-face semi-structured interviews with 15 Internet scammers operating in Cameroon. Both the empirical (Burrell, 2008) and theoretical (Akinladejo, 2007; Salifu, 2008) scamming literature explored why people become Internet scammers. The typical identified reasons include monetary rewards, socioeconomic and political problems (such as corruption, mismanagement, poverty, and unemployment), and affordable Internet in poor communities (Akinladejo, 2007; Ampratwum, 2009; Burrell, 2008; Walker, Adomi, & Igun, 2008). First, because the act of scamming is to swindle online buyers for their money, monetary reward is a plausible explanation. Indeed, many individuals motivated by monetary reward and who experience hardships from the socioeconomic environment do not become criminals. We address this question by focusing on an important issue not addressed in extant research: *Why is money a motivator for becoming an Internet scammer?* Moreover, the money explanation does not address how one becomes an Internet scammer. It is necessary to understand the stages and/or processes involved in becoming a scammer so that interventions can be at the earliest possible stage. Second, although Internet scams have become popular because of the Internet, researchers have not examined what makes computer-mediated communication (CMC) conducive to scams; that is, besides its features that facilitate anonymity and unlimited communication from anywhere and at any time. To explain our findings, we show how the problems we address relate to the relevant criminological theories. We also theorize that becoming a scammer unfolds through a series of stages.

On the question of why money motivates one to become a scammer, we find that the money is needed to socialize, enjoy an extravagant lifestyle, and become financially independent. Regarding how one becomes a scammer, we identify three stages. Stage 1 identifies the problems and negative emotions from individuals' pre-scamming activities that explain why they took their first steps toward scamming. Stage 2 identifies the associations, lifestyle preferences, and forms of misrepresentation, enabled and facilitated in CMC, as attributes that explain why individuals specifically became Internet scammers. Stage 3 identifies the justifications and subjective perceptions of anti-scamming deterrence measures that explain why individuals persist in committing Internet scams. We also show how these findings relate to dispositional and situational criminological theories. In this regard, our contribution suggests that none of the dispositional crime theories that focus on individuals' proclivity toward criminality, can adequately and specifically explain why people become scammers. This is because becoming a scammer is affected by problems, solutions, and preferences that are specific at the individual level, whereas the

explanations from theories are generic. Further, we suggest that, although situational crime theories (e.g., routine activities theory) attempt to explain why criminal acts occur, they cannot adequately explain why scamming occurs because they can neither explain the role of the offender nor the role of the computer-mediated environment in criminality. Thus, our findings highlight the need for context-specific theorizing. We further explain how such theorizing has implications for practice regarding combating Internet scams, for example, understanding the locales scammers operate from and how scammers subjectively assess deterrence measures within that locale before rolling out anti-scamming measures.

3.3 Internet Scamming and Previous Work

Internet scamming, also known as advance fee fraud, is used to swindle online buyers into making payments for nonexistent merchandise (Burrell, 2008). Although scams existed long before the Internet,[1] they have become pervasive because of the Internet. Before the Internet, scams were conducted in offline, face-to-face communications. There are variants of scams in different parts of the world (Salifu, 2008). Regardless, the different variants rely on a similar tactic of persuading an individual to make an advance payment for nonexistent merchandise. Although Internet scams come from around the globe (Glickman, 2005), it is generally assumed that most are perpetrated by scammers operating out of some West African countries. Researchers have argued that the social conditions because of the "paradox of plenty" causes "…resource-rich states outside the Western world to fall into impoverishment, conflict and corruption" (Peel, 2006 p. 2). The African countries most afflicted by Internet scammers' activities, such as Nigeria, Cameroon, Sierra Leone, and Ghana, are often cited as examples. Consequently, the prevalence of scamming (traditional and Internet) in these countries is often attributed to poor socioeconomic performance, rising unemployment, poverty, mismanagement, corruption, and lack of accountability and transparency (Ampratwum, 2009).

The Internet, however, has made advance fee fraud scams a global problem. While scholars attributed the emergence of scams to failed political regimes, they also viewed the Internet as providing a platform for Internet scammers (Peel, 2006 p. 2; Walker et al., 2008). Indeed, 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. Traditional face-to-face scams occur in a physical environment where the scammers are constrained by time, location, and physical appearance. Despite its benefits, the Internet is often

[1] Some researchers have argued that advance fee fraud scams originated in the 16th century (Peel, 2006). The example that is often cited is the "Spanish Prisoner scam": a wealthy merchant would be asked by a stranger to pay for the smuggling of a wealthy prisoner from prison in exchange for a reward that was never honored.

apportioned some blame for Internet scammers' activities (Akinladejo, 2007). The increase in Internet connectivity is assumed to serve two purposes. On one hand, it is an opportunity to connect and empower socioeconomically disadvantaged communities. Efforts by governments, nongovernmental organizations (NGOs), and individuals to increase the penetration of Internet access are being interpreted as opportunities for cybercrime in a West African context (Boateng, Olumide, Isabalija, & Budu, 2011). Conversely, it is a means to personal gain through illegitimate means (Boateng et al., 2011; Burrell, 2008). Researchers also assume that people choose scamming because legitimate channels are closed to them because of corruption (Peel, 2006). Accordingly, past studies relying on data from West Africa, emphasized monetary reward, socioeconomic and political problems, and Internet access as the main causes for becoming an Internet scammer. In other words, individuals are driven into scamming because legitimate avenues for success are closed to them. Importantly, although the explanations based on monetary reward, poverty, and increased Internet connectivity are plausible, they are also largely descriptive and not grounded in convincing empirical evidence. Moreover, as many individuals motivated by monetary reward, for example, do not choose to become criminals, the extant explanations cannot be the whole story regarding why people become Internet scammers. Importantly for this research, they do not explain how one becomes an Internet scammer.

With one exception (Burrell, 2008), most studies are based on secondary data taken from international agencies (Ampratwum, 2009) and reviews of published articles that relied on secondary or anecdotal data (Abia et al., 2010; Duah & Kwabena, 2015). For example, (Abia et al., 2010) examined why many teenagers were drawn into Internet scamming in Cameroon by interviewing school pupils who have scammer friends. Similarly, several recommendations for interventions to reduce Internet scams are based on secondary data (e.g., Walker et al., 2008). In contrast, (Burrell, 2008) interviewed actual Internet scammers ($n = 3$) operating in Ghana. Burrell (2008), however, stated that "Among those interviewed, there was no credible evidence that any of their scamming activities had resulted in financial gain" (p. 17). Therefore, although many scholars have attempted to study Internet scammers, it is questionable whether anyone has used successful scammers as subjects. Table 1 summarizes of the extant academic literature on Internet scamming (Appendix 2).

In summary, the existing explanations and the evidence on which they are based call for more studies on Internet scammers and their activities. Importantly, most scamming studies are either based on anecdotal evidence or on theories from sociology and criminology. In the next section, we discuss stage theories followed by a separate section on criminological theories. A stage perspective is important for understanding how one becomes an Internet scammer.

3.4 Stage Theorizing

Stages are defined as a set of categorically different, ordered states, which are similar in terms of cognitive, emotional, and behavioral features, but psychologically different from each other (Weinstein, Rothman, & Sutton, 1998). Stages are developed to understand how people change or how people behave (Schwarzer, 2008). In health psychology, stage theories have been widely applied to investigate health protective behaviors and stop unhealthy behaviors (Weinstein et al., 1998; DiClemente et al., 1991; Prochaska et al., 1994). Some examples include the transtheoretical model (Prochaska & Velicer, 1997), the precaution adoption process model (Weinstein & Sandman, 1992a), and the health action process approach (HAPA; Schwarzer, 2008).

The idea of stages may be intuitively compelling; that is, change occurs through a sequence of qualitatively different psychological factors and practices as individuals gradually adopt new behaviors (Sniehotta & Aunger, 2010). For example, to create a scamming advertisement, an Internet scammer must first write the advertisement and choose a preferred medium to post it. This suggests that many disparate factors or attributes are likely to influence behavioral change at different stages. However, most theoretical models of behavioral change (e.g., protection motivation theory and theory of planned behavior) are continuum models. They suggest that people can adopt new patterns of behavior with a single equation (Sniehotta & Aunger, 2010). For example, a small set of factors such as self-efficacy, outcome expectations, and intentions are used to predict behavior in continuum models.

In developing stage models, the underlying assumption is that interventions or recommendations to change a behavior will be tailored to the needs of the individuals or behaviors at a particular stage. Further, recommendations should also consider that different categories of people may need different kinds of help. Stage researchers (Weinstein & Sandman, 1992b; Weinstein et al., 1998) have recommended stage criteria that consider issues such as whether the movements among the stages are sequential. Do the variables that predict progress from stage to stage vary or do they remain the same? Do people at different stages have different behavioral patterns? However, they do not expect a single study to address all these issues.

3.5 Criminological Theories

In this section, we discuss the relevant theories to our study. This study is inductive; therefore, we did not rely on any theories when collecting and analyzing the data. We review these theories because different portions of our findings are relevant to some aspects of these theories at different stages. Understanding why people engage in a particular crime and why people commit particular crimes is a prelude to developing strategies to control the

behavior. Often overlooked in the literature on IS security is the fact that most criminological theories are either situational or dispositional and are not adequately and specifically applicable to the IS context. Traditionally, criminologists have explained criminality through the dispositional attributes that are assumed to explain why some individuals are born with, or come to acquire, a "disposition" to offend (Clarke, 1983p. 228). For example, the dispositional attributes introduced by classical criminology emphasize biological factors (e.g., genetic differences) that affect criminality. Contemporary crime theorists subsequently introduced psychological (e.g., personality and upbringing) and sociological (e.g., from a gang subculture or poverty) factors. A dispositional approach to criminality is influenced by previous personal history (Clarke, 1983; Gottfredson & Hirschi, 1990).

However, in 1947, Edwin Sutherland introduced the idea of explaining criminality through dispositional and situational factors (Sutherland & Cressey, 1947). Sutherland argued that crime was either historical or situational. Clarke (1983) specified situational crime as crime that is influenced by environmental factors surrounding the crime scene. Clarke further argued that dispositional factors alone make it hard to implement actions that reduce opportunities for crime at particular times and places. Therefore, the criminal act should be studied as distinct from the disposition to commit a crime because it does not "result simply and inevitably from the presence of a criminally disposed individual" (Clarke, 1983, p. 229). Examples of situational studies include crime-specific studies on shoplifting (Walsh, 1978), vandalism (Clarke, 1978), and burglary (Brantingham & Brantingham, 1975). Situational studies on burglary, for example, suggest that crime increases with the availability and portability of valuable consumer goods. Studies on victimization suggest that this outcome is also affected by the lifestyle choices of victims (Hindelang, 1976). Although there seems to be a consistent and predictable relationship between crime and situational factors, the relationship is not causal. Nonetheless, in explaining criminality, it is necessary to also explain the criminal act and how it affects criminal behavior.

The criminological theories discussed include the general strain theory (GST; Agnew, 1985; Agnew, 2001), social learning theory (SLT; Akers & Jennings, 2009), general deterrence theory (Nagin, 1998; Tonry, 2008), rational choice theory (RCT; McCarthy, 2002), neutralization theory (Sykes & Matza, 1957), and routine activities theory (RAT; Cohen & Felson, 1979).

3.5.1 Deterrence Theory

In the eighteenth century, the emergence of the classical theory was seen as a liberal reform to the criminal justice system. This reform was pioneered during the Enlightenment era by utilitarian philosophers Cesare Beccaria (1738–1974) and Jeremy Bentham (1748–1832). They argued that, because people fear pain, given a choice, they will choose pleasure. In other words, people will choose crime whenever its benefits are higher. Classical theorists viewed criminals as calculating the risks and rewards of committing crimes. Accordingly, they

argued that a fair justice system in which punishment is certain and swift will deter future crime if the pain outweighs the gains (Lilly, Cullen, & Ball, 1989). Although deterrence owes its intellectual origins to Beccaria and Bentham, it owes its empirical roots to (Gibbs, 1975; Tittle, 1969). These scholars used official data (e.g., police and court records) to assess whether punishment certainty (incarceration/arrest) and punishment severity (incarceration length) reduced the likelihood of future crime (Paternoster, 1987; Schell-Busey, Simpson, Rorie, & Alper, 2016).

Traditionally, deterrence theory suggests that certainty, severity, and celerity of punishment have a deterrence effect on offenders and would-be offenders. The deterrence effect functions in two ways: through specific deterrence, where the prescribed punishment is designed to deter only the individual offender and through general deterrence, where the punishment is designed to deter the general population from engaging in crime. The deterrence effect is often publicized to make potential offenders aware of the futility of participating in crime (Nagin, 1998; Tonry, 2008).

The major criminological reviews on deterrence theory have typically suggested that increases in punishment have overall marginal deterrence effects; however, the available evidence is also inconclusive, contested, and dependent on the specific crime (Tonry, 2008; Naggin, 1998). Although deterrence theory has been extensively studied (Nagin, 1998), research on deterrence has primarily focused on traditional crimes (Schell-Busey et al., 2016). Consistent with what Bentham and Beccaria believed, some evidence suggests that certainty and celerity of punishment are more important than severity (Tonry, 2008).

Whereas some deterrence research is based on the effect of formal (legal) punishment for crime (i.e., objective deterrence; Schell-Busey et al., 2016), other deterrence research is based on how offenders subjectively assess the threat of sanction (perceptual deterrence; Gibbs, 1975). In general, perceptual researchers have found criminality to be lower among individuals who perceive the threat of punishment to be high (Grasmick & Bursik Jr, 1990; Paternoster & Simpson, 1996)

Such findings are not very helpful; of greater interest, would be how the specific deterrence measure yields a deterrence effect. Criminologists have noted that this depends on the specific form of the crime, how it is perpetrated, the process by which people learn to commit the crime, and how offenders perceive the deterrence measures.

Consequently, even though deterrence research has reported negative associations between crime rates and sanction levels (Sampson & Cohen, 1988; Kagan, 1989; Levitt, 1996), it is difficult to generalize from these studies. Knowledge about the factors that affect the efficacy of a deterrence measure also depends on the nature of the crime and of the offenders (Nagin, 1998). This suggests a bias toward studies with fine-grained details; the details from these kinds of studies provide relevant knowledge for policymakers (Tonry, 2008). Because offenders' decisions to commit a crime are influenced by their specific

contexts, criminologists view the macro level (e.g., economists and econometricians) as being incapable of explaining how offenders perceive the deterrence measures (Tonry, 2008). Deterrence measures that fail to consider offenders' views can lead to the adoption of mistaken policies. The implementation of some deterrence measures includes well-publicized police crackdowns (Sherman & Ross; Nagin, 1998; Tonry, 2008). Criminologists have generally found such interventions to be successful in generating an initial short-term deterrence effect (Sherman & Ross; Nagin, 1998; Tonry, 2008). In some cases, the deterrent is effective through informal sanctions, such as the fear of shame, for example, because offenders fear the social stigma of having a criminal record.

In summary, the effectiveness of deterrence measures is context dependent and influenced by offenders, how the crime is committed, and knowledge of the certainty, severity, and celerity of the implementation of the measures. The existing evidence from the criminological literature is inconclusive.

Similarly, in the IT context, findings on the deterrence effect are also inconclusive. Deterrence theory is among the most widely studied theories in IS (D'Arcy & Herath, 2011; Siponen & Vance, 2010; Willison & Siponen, 2007). Since (Straub Jr, 1990) introduced deterrence to IS security research, several studies have been conducted investigating the deterrence effect (D'Arcy, Hovav, & Galletta, 2009a; D'Arcy & Herath, 2011; Pahnila, Siponen, & Mahmood, 2007; Siponen & Vance, 2010). The IS scholars have tested its ability to predict employees' compliance and noncompliance with IS security. Straub (1990) used security policies, security staff hours, and technical controls as proxies for deterrence to investigate their effectiveness in controlling computer abuse. While Straub found the measures to reduce computer abuse, many other studies have yielded different results.

At the individual level, (D'Arcy, Hovav, & Galletta, 2009b) found perceived severity reduces IS misuse intention, but perceived certainty does not. Consistent with D'Arcy et al., (2009b), Cheng, Li, Li, Holm, & Zhai, (2013) reported that the severity of sanctions significantly affects employees' IS security policy violation intentions, but certainty of sanctions does not. Cheng et al., additionally reported that the threat of a harsh penalty if caught motivates compliance. Herath & Rao, (2009) found that certainty of detection has a positive effect on the intention to comply with IS security policies, but severity of penalty does not. Other scholars reported that deterrence countermeasures did not have a significant influence on employees' intention to comply with security policies (Lee, Lee, & Yoo, 2004; Pahnila et al., 2007; Siponen & Vance, 2010). Thus, similar to deterrence research in criminology Paternoster (1987), IS research on deterrence is hindered by mixed results.

3.5.2 Social Structure Theories: Strain Theory

The Chicago School has had a significant influence on criminological thinking. Several pioneers from the Chicago School emerged in the 1920s and 1930s,

including Edwin Sutherland, Robert Merton, Clifford Shaw, and Henry McKay. The emergence of the Chicago School was influenced by the changes occurring in American society. There were major demographic shifts occurring in American inner cities due to mass migration. The city of Chicago was at the heart of these demographic changes, resulting in two major criminological traditions, both focusing on the social context: strain theories and subcultural theories of crime.

Wickersham Commission, Shaw, & McKay (1931) pioneered the ecological approach to crime in Chicago during the 1920s at a time of major transitions and mass poverty. Shaw and McKay viewed crime as emerging from the prevailing cultural norms and values existing in lower-class culture. Consequently, they rejected the prevailing racial and cultural explanations at the time. Instead, they argued that the ecological conditions of the city itself were the cause of delinquency. Relying on case material from court and police records, Shaw and McKay studied the attitudes of offenders in relation to the community, the play group, the gangs, and the family.

They found that areas with low crime rates were associated with conventional practices, such as good homes, respect for the law, and church attendance. Such values, however, were absent in areas with high crime rates. Instead, the youths in the high crime areas were exposed to conflicting moral values. Shaw and McKay also observed that delinquency correlated with economic and social conditions, such as poverty, poor health, and poor housing. Financially deprived and living in poor neighborhoods, lower-class youths choose crime as a means for economic achievement, socialization, and prestige. In contrast, because middle-class youths have access to mainstream cultural norms (from attending schools and church), they were exposed to socialization process practices that promote conventional attitudes and behaviors. This ecological approach paved the way for other theoretical perspectives, such as the strain approach to crime. Regardless, Shaw and McKay had relied on court and police records, which changed from time to time and varied from one neighborhood to another. Thus, their theory was heavily criticized.

3.5.2.1 General Strain Theory

The first strain theory, developed and made popular by Robert Merton, was based on Durkheim's pioneering work. Emphasizing the consequences of a breakdown in social control, Durkheim proposed that pressures toward the formation of delinquent subcultures are induced by the inability of the lower-class youth to achieve culturally defined ends through legitimate means (Ohlin & Cloward, 1960). In such situations, the outcome is anomie – normlessness or lawlessness from a breakdown in social order.

Similarly, Merton argued that anomie does not develop from only a breakdown in goal achievement alone. Merton proposed that anomie develops from a breakdown between goals and the legitimate means of achieving them (Cloward & Ohlin, 1960). From studying crime in impoverished Chicago neighborhoods, Merton concluded that the anomic conditions within the

American society that give rise to these strains are culturally defined goals (e.g., wealth accumulation, success, and power) and socially approved means (e.g., hard work and education). Merton's theory focused solely on the utilitarian aspects of crime.

Scholars, notably Albert Cohen, criticized Merton's theory of anomie for not addressing non-utilitarian aspects of crime, which may be unrelated to success goals, such as violence, vandalism, or murder (Siegel & Senna, 1985). To address the criticisms from Merton's theory, Agnew, 1985; Agnew (2001) conceptualized a GST, focusing individual level strains and emphasizing a social psychological perspective. The GST focuses explicitly on negative relationships in which people are not treated as they want to be treated and on negative events and conditions disliked by people. Agnew specifically emphasized that strains may cause many emotions, such as fear, humiliation, frustration, and anger, of which anger is most applicable to crime. Departing from Merton's narrow focus, Agnew argued that strains may come from many sources, not just from a failure to achieve economic success (Agnew, 2001, 2002; Hay & Evans, 2006). Examples of strains associated with crime include parental rejection, unfair discipline, child abuse, bullying, negative school experiences, marital problems, criminal victimization, and homelessness (Agnew, 1992). Because strains may make it impossible for some individuals to achieve their life goals (e.g., monetary success, social status, and power), some people use crime to cope. The GST also claims that strains may foster the social learning of crime (Agnew, 2006).

Even though GST stipulates that certain strains (e.g., anger) are more applicable to crime, it also acknowledges that most strained individuals do not cope through crime. Further, GST also identifies the factors that increase the likelihood of criminal coping: possessing poor coping skills and resources, low levels of conventional social support, low social control, associating with criminal others, holding beliefs favorable to criminal coping, and viewing the costs of criminal coping as low and the benefits as high (Akers & Jennings, 2009, p.335). Therefore, GST proposes that the strained individuals who engage in crime lack legal coping strategies (Akers & Jennings, 2009). Further, strain-producing negative emotions are more likely to result in crime when the people experiencing the strains see these strains as high in magnitude, unjust, and associated with low social control (Agnew, 2001).

Although IS scholars have not examined the role of strain in IS security behaviors, several criminological studies have found empirical support for the central propositions of GST. Using data from undergraduate students, Broidy (2001) reported that strain-induced anger significantly increased the likelihood of deviant outcomes. Some researchers examined the role of stressors on criminal behavior and reported that perceived discrimination predicted crime and substance use (Eitle, 2002). People with more stressful life events are more likely to become criminals (Eitle & Turner, 2003). Empirical studies on GST also indicate that the effects of strain on crime are often partly explained by negative emotions as well as by social control and social learning (Jang & Rhodes, 2012).

3.5.2.2 Neutralization Theory

Prior to Sykes & Matza (1957), Albert Cohen (1955) articulated a subcultural theory focusing on the relation between criminal behavior and social class structure. Cohen argued that delinquent boys, unable to climb up the social ladder, reject mainstream culture and create their own subculture. Challenging this view, Sykes and Matza (1957) argued that delinquents do not necessarily reject mainstream culture when they join a subculture. They argued that many delinquents view their delinquency as wrong from their upbringing and interactions; accordingly, delinquent boys share similar values and norms as other members of society and experience guilt and shame for their crimes.

Refining this idea, Matza (1961) argued that some delinquents are in a state of drift between a conventional lifestyle and a delinquent lifestyle. Thus, rather than being opposed to mainstream culture, many delinquents adhere to the norms of mainstream society but render them ineffective through techniques of neutralization. However, mainstream norms serve as checks on their behaviors (Conklin, 2013; Matza & Sykes, 1961). Thus, delinquents invoke techniques of neutralization to minimize their commitment to the law and to the expectations of others by drifting in and out of the moral values of the mainstream culture (Matza & Sykes, 1961). Sykes and Matza (1957) identified five techniques of neutralization that delinquents use prior to violation of the law: denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and appeal to higher loyalties (Table 2). Matza (1964) added that youths are drawn into delinquency because of its rewards or values, which can include an adventurous lifestyle (of excitement, thrills, or kicks).

To understand why employees violate security policies (Puhakainen & Siponen, 2010), IS scholars have found that neutralization techniques are often stronger than sanctions (Siponen & Vance, 2010). When neutralization techniques are invoked, even non-malicious employees can deliberately violate security policies (Guo, Yuan, Archer, & Connelly, 2011; Siponen & Vance, 2010). Siponen and Vance (2010) examined specific neutralization techniques and found them to be more effective predictors of IS security policy violation than sanctions from general deterrence theory. (Harrington, 1996) identified denial of responsibility as a significant predictor of employees' computer abuse judgments. Although Siponen and Vance (2010) reported that neutralization techniques have similar effects, (Barlow, Warkentin, Ormond, & Dennis, 2013) reported that the effects of different neutralization techniques depend on the particular security violation.

In criminology, findings for neutralization have been mixed (Maruna & Copes, 2005). Scholars have attributed the mixed results to researchers not tailoring specific neutralization techniques to specific behaviors (Morris, Johnson, & Higgins, 2009). In their review of 50 years of neutralization theory, Copes and Maruna (2005) argued that researchers continue to utilize neutralization in its original form, instead of refining neutralization to suit

specific problems. The authors also argued that neutralization is probably better suited to explaining persistence in crime than the onset of crime.

TABLE 2 Techniques of neutralization

1	The denial of responsibility	The offender denies being responsible for the crime, claiming instead that the crime is the result of external forces beyond the offenders' control such bad friends or unloving parents.
2	The denial of injury	The offender can argue that no one was hurt; no harm was done; or the victim can afford it. Thus, the offender uses linguistic devices to undermine the criminal act.
3	The denial of victim	The offender will argue that the victim deserves it; the injury is not an injury but a rightful retaliation.
4	The condemnation of condemners	Offenders shift the focus from their deviance to the motives and behaviors of those who disapprove their crimes. The condemners (e.g., police, teachers, or lawmakers) are hypocrites or criminals in disguise. In this fourth technique offenders change the conversation from their crimes by attacking others
5	The appeal to higher loyalties	Offenders argue they are caught up between meeting the demands of their smaller groups (friends, siblings, or gang) at the cost of violating the law and respecting general social norms. The law is violated not because it is unimportant, but because of other more pressing demands involving higher loyalty.

3.5.2.3 Social Learning Theory

Akers' SLT emerged as an extension and a reformation of Sutherland's differential association theory. The work by Shaw and McKay was the foundation for Edwin Sutherland's classic differential association theory. Shaw and McKay concluded that the social roots of crime are transmitted in a similar fashion as language and other forms of social behaviors (Lilly et al., 1989). In turn, Sutherland argued that some social groups are organized in ways that either encourage or discourage crime. Sutherland presented his theory as a general theory of crime; that is, all forms of crime involve social learning.

According to Sutherland, criminals and non-criminals are separated by the content of what they have learned; people learn to commit crime just as they learn to play baseball or paint. Following a life-history study on Chic Conwell, a professional thief, Sutherland (1937) came to a more general conclusion that differential association with thieves is the critical factor determining whether one becomes a pickpocket, a shoplifter, or a con artist (Siegel & Senna, 1985). Differential association theory was, however, not widely accepted in sociology and criminology. Scholars criticized the theory for having too broad constructs that cannot be empirically validated (Burgess & Akers, 1966).

Following Sutherland, Akers developed the SLT, equally positioning it as a general theory of crime. Drawing from Albert Bandura (1977), Akers

suggested learning occurs in a social context through direct experience, observation, imitation, and modeling (Crain, 2015). Akers & Jennings (2009) reformulated Sutherland's nine statements of learning into seven (Table 3). The SLT stresses that the process of learning about crime occurs through four central concepts: differential association, definitions, differential reinforcement, and imitation (Akers & Jensen, 2006). Although associating with criminals increases a person's likelihood of becoming a criminal, mere association is not enough. Instead, the associations must be frequent, intimate, and of long duration. In addition, a person must also learn the definitions that are favorable to crime and prefer them over definitions emphasizing conformity with the law. A definition is an orientation and attitude toward a given behavior. Criminals are assumed to have favorable definitions toward crime. Differential reinforcement emphasizes the benefits, such as peer approval, for participating in criminal behavior. Through imitation, a person observes and follows the behavior of another. Regardless, SLT has similarly been criticized for been too broad and for failing to specify whether an individual becomes a delinquent before associating and learning from other delinquents. In addition, SLT does not specify what is involved in the learning.

TABLE 3 Seven principles of social learning (Akers & Jennings 2008, p. 324; Burgess & Akers, 1966)

Statement numbers	Descriptions
1	Criminal behavior is learned according to the principles of operant conditioning (reformulation of Sutherland's Principles 1 and 8).
2	Criminal behavior is learned both in nonsocial situations that are reinforcing or discriminative and through that social interaction in which the behavior of other persons is reinforcing or discriminative for criminal behavior (reformulation of Sutherland's Principle 2).
3	The principal part of the learning of criminal behavior occurs in those groups which comprise the individual's major source of reinforcements (reformulation of Sutherland's Principle 3).
4	The learning of criminal behavior, including specific techniques, attitudes, and avoidance procedures, is a function of the effective and available reinforcers, and the existing reinforcement contingencies (reformulation of Sutherland's Principle 4).
5	The specific class of behaviors which are learned and their frequency of occurrence are a function of the reinforcers which are effective and available, and the rules or norms by which these reinforcers are applied (reformulation of Sutherland's Principle 5).
6	Criminal behavior is a function of norms which are discriminative for criminal behavior, the learning of which takes place when such behavior is more highly reinforced than noncriminal behavior (reformulation of Sutherland's Principle 6).
7	The strength of criminal behavior is a direct function of the amount, frequency, and probability of its reinforcement (reformulation of Sutherland's Principle 7). (pp. 132–145

Although IS scholars have only begun studying the role of SLT in crime (Lowry, Zhang, Wang, & Siponen, 2016; Young & Zhang, 2005) in the criminology literature, SLT has been the subject of many empirical studies. Researchers have tested the principle of differential association on gang membership (Decker, Pyrooz, Sweeten, & Moule Jr, 2014; Kissner & Pyrooz, 2009) and in the context of offline bullying behaviors (Moon et al., 2010; Espelage et al., 2000). In online settings, Hollinger (1993) reported that friends' involvement in computer piracy increased a respondents' involvement in computer piracy. Similarly, Skinner & Fream (1997) also reported that the strongest predictor of computer crime (computer piracy, hacking, infecting computers with viruses) is differentially associating with friends who participate in computer crime. Some researchers, however, have reported findings that are inconsistent with the principle of differential association. In a study that examined the onset of bullying behavior, Moon, Hwang, & McCluskey, (2008) did not find support for the principle of differential association theory.

3.5.2.4 Rational Choice Theory

The RCT explains how people make decisions when faced with choices. The RCT has been widely applied to study individual, social, and economic behaviors in many contexts (McCarthy, 2002). The earlier economic approaches to crime assumed that rational choice is mainly influenced by self-interest. This approach predicts that crime is reduced by reducing the monetary benefits of crime and increasing the severity of punishment (Schmidt & Witte, 2013). However, a broader approach to RCT adopts a wider range of preferences (Eide, Aasness, & Skjerpen, 1994). A broader approach to RCT views the decision to act as involving individuals' preferences, attitude toward risk and time discounting, and costs and benefits that affect the decision to offend (McCarthy, 2002). Thus, a rational choice decision is affected by individuals' preferences and orientations toward present versus future outcomes. A preference can involve forgoing an immediate benefit for greater future compensation. However, preferences typically do not refer to outcomes; most outcomes are uncertain and are unlikely to be realized (McCarthy, 2002). Preferences are also affected by the available information. Although people prefer their decisions to be guided by complete information, most decisions are made with incomplete and/or inaccurate information. Nonetheless, rational actions are those that show consistency between people's preferences and their choices. McCarthy (2002) argued that a rational choice approach is not a theory of cognition, as people do not always think in ways that are typically associated with rationality (e.g., reasoned, thoughtful, and reflective), and most decisions that people make are not based on literal calculations.

The rational choice approach to crime only provides an account of how people's preferences affect their choices. Thus, the rational choice approach to crime does not explain the source of people's preferences. This presents a sharp contrast with other, typically dispositional crime theories, such as SLT and GST. However, the rational choice approach relates to other crime theories that focus

on the decision to commit a criminal act, such as the RAT (Felson & Cohen, 1979) and the reasoned-offender approach (Cornish & Clarke, 1986). While there are criticisms against RCT, McCarthy (2002) argued that a broader approach to RCT addresses these criticisms because they stem from confusion about its key concepts, premises, and predictions.

3.5.2.5 Routine Activities Theory

Unlike dispositional theories, situational theories (e.g., RAT or lifestyle theory) do not associate crime with structural problems (e.g., poverty, inequality, and unemployment) or with offenders' prior histories. Situational theories suggest that crime cannot be committed unless there are opportunities to break the law. The RAT was first introduced by Cohen and Felson (1979) and is a situational theory that views crime as a function of people's everyday behavior. Shoplifting, burglary, and employee theft are some examples of crimes explained by RAT. Opportunities for crime occur when people's daily routines make them suitable targets by motivated offenders either because they are inadequately protected (e.g., a property) or because they cannot protect themselves (e.g., a vulnerable person; Conklin, 2013).

The RAT focuses on three elements: motivated offenders, target suitability, and the absence of guardianship. According to Tonglet (2002), motivated offenders have moral beliefs that support theft and the belief that the rewards from theft outweigh the risks. Thus, motivated offenders commit crimes when they encounter desirable merchandise that is unprotected and easy to steal. An abundance of merchandise also increases opportunities for theft (Stack, 1982). A suitable target is a property or person that is visible, vulnerable, and accessible to offenders. The absence of guardianship proposes that a target lacks the means and resources to fend off or avoid victimization; for example, they cannot call for help (Mustaine & Tewksbury, 2007). Guardianship refers to the extent to which people protect (or not) their property during their daily lives, for example, not switching off the car when shopping in low temperatures. According to RAT and the lifestyle approach to crime, the absence of guardianship from homeowners (e.g., working long hours away from home or taking frequent and long vacations) can result in increases in home burglaries.

The RAT is primarily a macro theory of victimization focusing specifically on individuals who are suitable targets for motivated offenders. However, because it is a situational theory, the RAT attempts to specify the minimal conditions necessary for a crime to occur and to focus attention on elements of a crime independent of the offender. Whereas the RAT provides characteristics of the situations, targets, or victims of crime, it only notes that the offender must be motivated to seize the opportunity.

3.6 Methodology

We used an interpretive approach to understand how one becomes an Internet scammer. Several researchers have reported on the appropriateness of the interpretive approach to studying the complex interaction of people and computers within their social settings (e.g., Myers, 2013; Orlikowski & Baroudi, 1991). To code the interview data, we applied the open and selective procedures associated with grounded theory (Glaser, 1978). Even though open and selective coding procedures are often associated with grounded theory (Glaser, 1978), we only used them as a means of performing data analysis (Urquhart, 2012). Accordingly, we make no claim that this is a grounded theory study. Open and selective coding procedures are well established methods for analyzing qualitative data (Urquhart, Lehmann, & Myers, 2010). The interpretive approach allowed us to develop theoretical explanations inductively and then to integrate them with the relevant existing literature.

3.6.1 Data Collection

This study is based on semi-structured interviews conducted with Internet scammers operating in Cameroon. The interview data for this study was collected in two field trips. The planning before and during the interviews was facilitated by a local acquaintance. Getting to interview scammers has proven difficult. The second author works with the National Bureau of Investigation and knows that even Interpol has not been able to go undercover and do interviews with scammers. Therefore, getting access to the scammers requires inside contacts. We relied on a local acquaintance introduced to the first author by his friend[2] who owned a cybercafé. The first author is a Cameroonian, and this was a necessary requirement to meet and interview the scammers because they were more suspicious that a Westerner could be working for the authorities.

The first interviews were conducted in March 2014, and five Internet scammers were interviewed. These first interviews, which focused on why subjects became Internet scammers, were also an opportunity to identify problem areas for more probing. The first three interviews involved individuals who have been practicing Internet scams for over ten years. These individuals were aged between 35 and 42. In contrast, the last two individuals had at most five years of experience (Table 4) and their ages ranged between 25 and 30. Our goal was to use theoretical sampling to select the subjects. We tried to achieve

---

[2] The first author's friend knew many scammers, however, because he was not friends with them, they would not open up or even concede to him that they are scammers. Thus, a local acquaintance (who is not and has never been a scammer), who is a friend to some of the scammers interviewed for this study, was in a better position to approach them. Because he also works as a community organizer, our local acquaintance knew the right people to negotiate with contacting other scammers that he was not close with.

this during the first field trip by deliberately choosing Internet scammers with varying years of experience.

TABLE 4 Subjects pre-scamming activities and years of Internet scamming experience

Subjects	**Types of previous economic activities**
1 (equal to or more than 10 years)	Hawking
2 (equal to or more than 10 years)	Managing garage and secondhand car parts shop
3 (equal to or more than 10 years)	Managing video club
4 (less than or equal to 10 years)	Job-seeker
5 (less than or equal to 10 years)	Attending school

The second round of interviews occurred in January 2015 with 10 Internet scammers. Although we had also planned to interview Internet scammers whose years of experience varied significantly (e.g., over ten years, between five and ten years, and less than five years), we only succeeded in interviewing individuals with under ten years of experience. In total, the data comprises 15 different Internet scammers and each subject was only interviewed once. With one exception, all the subjects with less than 10 years of experience were attending either high school or university at the time they became Internet scammers. The one exception had completed vocational training and was a job-seeker. The subjects with equal to or more than 10 years of experience were living with their guardians and were financially dependent on them. In general, the subjects with less than or equal to 10 years of experience were in their mid-to-late twenties at the time of the interviews.

We were led to believe by the local acquaintance that all subjects have made money from Internet scamming. During the interviews, the scammers corroborated this assertion. Each interview lasted between 45 and 65 minutes. The subjects all gave permission for their voices to be audio recorded, but anonymously. All the individuals we could interview and made aware of were men. We conducted the interviews at secure locations chosen by the subjects. The subjects were offered a small reward for participating and promised strict confidentiality of their anonymity.

The semi-structured interviews were an opportunity to learn about the many issues before they became Internet scammers and why they continue practicing Internet scams. The interviews started with questions about subjects' key activities and experiences before scamming, their respective ages and immediate activities when they heard or considered scamming, and how they became Internet scammers including the learning process (what was learned, how, where, and with whom). We also asked about their reasons for giving up these pre-scamming activities for scamming. Subjects were also asked why they are Internet scammers, for example, why continue and why not quit?

3.6.2 Data Analysis

The transcription and coding processes occurred simultaneously. The techniques of open and selective coding were applied in coding the data (Urquhart et al., 2010). Open and selective coding procedures are designed for generating theories based on interviews or observations (Strong et al., 2014; Urquhart, 2007). The data analysis involved coding the data to indicate the meaning of particular portions of the interview data at the sentence and paragraph levels (Myers, 2013). The goal was to identify key themes pertaining to how one becomes an Internet scammer.

3.6.3 Findings

This section summarizes the findings. Each chunk of quote from the subjects includes issues that are relevant to the different stages. For ease of reading, all the relevant transcripts are in the appendix (see appendix 2). The quotations in appendix 2 are organized as the findings presented here. Nonetheless, the findings present vivid descriptions from the subjects. The findings suggest that subjects with less than five years of scamming experience learned from their friends, whereas subjects with ten years and above learned opportunistically from random scammers. In addition, subjects with less than 5 years of experience were attending school (including teenagers), unemployed, and lacked an independent source of income when they became scammers. In contrast, subjects with equal to or more than 10 years of experience were financially independent and married with children. These differences are summarized in Table 6 in appendix 2. Whereas the subjects with more than or equal to 10 years of experience had conventional businesses before they were scammers, the current trend is teenagers becoming scammers, for example, through their friends. We view these differences as representing a generational gap in how people have become Internet scammers. Accordingly, we categorize Subjects 1, 2, and 3 as belonging to the old generation of Internet scammers and the rest as belonging to the new generation of Internet scammers.

3.6.3.1 Stage 1: Origin of the Problem

Loss of business income

The origin of the problems of the old generation subjects is the loss of business income, which threatened their financial independence. The three old generation subjects were engaged in different business activities: Subject 1 was a hawker, selling exotic insects to Western tourists; Subject 2 was a garage owner and secondhand car parts dealer, buying his merchandise from overseas suppliers; and Subject 3 owned a local 'video club' (a local cinema). However, problems emerging from their business models (Subject 3), interactions with their business customers (Subject 1), suppliers (Subject 1), and local tax authorities threatened their business incomes.

Subject 1 sold his merchandise to Western tourists visiting Cameroon. In addition to hawking from one place to another, Subject 1 also relied on a snowball approach. He asked his customers to recommend their acquaintances who need his merchandise. His initial contacts were through face-to-face interactions with the tourists visiting Cameroon. Over time, through snowballing, he had overseas customers calling in and later emailing him from Western countries. His main problem was that his overseas customers wanted him to sell at "unreasonably low selling prices."

Subject 3 had been managing his 'video club' business (i.e., a local cinema) since he dropped out of secondary school. His video club showed movies from a 20-inch television screen at a price of CFA 50 FRS for children and CFA 100 FRS for adults. However, changes in the business environment negatively affected his business income, leading to his business's eventual demise. These changes included the emergence of cheap DVD players and cable television. However, Subject 3 blamed his problems on the entry of cheap products into the market and the fact that he was still required to pay taxes.

Subject 2 claimed he was scammed by an overseas supplier who did not supply the merchandise he had pay for in advance. He was very angry that after university, he had to settle for a "dirty business." He was also very angry about the tax officials who wanted bribes to do their jobs; for example, he reported that tax officials assigned him to a higher tax category and wanted a bribe before they would reclassify him into a lower tax category. Subject 2 felt that, because his income was small, he rightfully belonged to a lower tax category. He was also angry at the corruption in the system as a whole for allowing people with less skills and qualifications to flourish because they had "god-fathers," while he did a job he did not like. Such comparisons, coupled with his negative experiences with some tax officials and an overseas supplier, filled Subject 2 with anger and frustration.

Friends become Internet scammers

The origin for the new generation subjects' problems can be traced to when their friends became Internet scammers and they chose to continue socializing with these friends, for example, accompanying their respective scammer friends to places where subjects became exposed to the extravagant lifestyle of scammers, such as nightclubs and social events. In such places, their scammer friends were among the most popular attendees and often would show-off, for example, offering to buy drinks for everyone. In other settings, they want to own the latest technological gadgets. At this point, subjects' financial expenses were covered by their scammer friends.

Although subjects were enthralled and overwhelmed by this lifestyle, they soon realized that their respective scammer friends wanted them to take charge of their own financial expenses. Not yet scammers, the new generation subjects could not afford the expenses they had been witnessing without becoming scammers themselves. Their scammer friends, however, pressured them to also become scammers and financially sponsor their love of the scammer lifestyle.

That would mean a complete change from their dominant pre-scamming activities.

Before they were exposed to scammers and their lifestyle, most new generation subjects were financially dependent on a guardian. Six were attending school or university and four had graduated but were unemployed. Among the four graduates, one had further studied for a professional diploma in information technology. Like most teenagers in Cameroon, they described themselves as "financially broke" (e.g., Subject 7). However, they loved the scamming lifestyle to which they had been exposed. Thus, subjects began seeing and complaining about problems in their lives they, hitherto, did not complain about. For example, they complained about poverty and unemployment because these are common and obvious problems in the country. Subjects complained about the high rates of unemployment and the uncertainty about getting a job upon completing school. Indeed, four subjects stated that they were unemployed jobseekers. The others, however, lacked any professional work-related skills and were not jobseekers. Moreover, the most salient concern after their friends became scammers was loneliness from losing their friends to scamming.

In summary, analysis of subjects' problems suggests that loss of business income is the main problem that affected old generation subjects' pre-scamming activities. This problem resulted in three negative emotions (anger, revenge, and disillusionment) that influenced their decisions to find an alternative means to make money. For the new generation subjects, the main problem identified was that friends became Internet scammers. This problem resulted in a negative emotion, loneliness, and a positive experience when subjects became exposed to the lifestyle of scammers and loved the lifestyle. However, because they loved the lifestyle, subjects were respectively peer pressured by their scammer friends to become financially independent by also becoming Internet scammers.

3.6.3.2 Stage 2: The Solution

Context of the solution

The old generation subjects felt the solution to their respective problems was finding alternative or supplementary sources of income. Subjects 1 and 2 were disgruntled that, on one hand, "greedy customers" and a "dishonest supplier," respectively, and, on the other hand, a corrupt system was negatively affecting their business income. Subjects 1 and 2 had come to the following conclusions, respectively:

- conventional work does not pay;
- those who attempt to work hard end up disrespected and disappointed; and
- the system is about cheating.

Therefore, to solve their problems, each subject scouted around learning from what others were doing to make quick money.

Subject 3 had also concluded that it was time to close his business and start something new. He started working at a cybercafé; however, the pay was too low to meet his family needs. He also viewed the job as simply a short-term fix until he could be owner manager again. In addition, a friend who sold insects to Westerners introduced him to the business, and this became another source of income for him. While working at the cybercafé, Subject 3 observed scammers committing Internet scams, and he became interested.

The new generation subjects, realizing they had to choose between their conventional activities and becoming Internet scammers, came up with reasons (unemployment, poverty, fear of being lonely, and love of the lifestyle) that choosing the latter was a better decision. However, these problems became imminent and prominent only after they experienced the scamming lifestyle and were pressured by their scammer friends to become financially independent.

The solution: Learning scamming and becoming Internet scammers

Subjects resolved to address their different problems by first learning how scams are committed and then committing Internet scams. For the old generation subjects, learning involved opportunistically observing other scammers at cybercafés (Subject 1). It also involved hearing tales from other scammers, searching online for more information, and learning scamming through trial and error. In contrast, the new generation subjects learned from their friends who became Internet scammers. Typically, subjects learned how to perform one scam before applying their skills to other types of scams. The most common scams that subjects learned and practiced include pets, dating, plantation, and fertilizer scams. Examples of what subjects learned include:

- Using Facebook to advertise scams: The new generation subjects primarily learned to commit scams through Facebook. Scammers like its mode of communication, which they said is faster in comparison to communication by email. This is because Facebook enables live chatting, which reduces the time to response with a potential victim. Unsuccessful scams are determined more quickly so that subjects can focus on new targets.
- Relying on prewritten letters: First, this is to reduce the risks of mistakes that can reveal that a supplier is actually a scammer. Second, the potential victims typically reply to a scamming advertisement with similar questions and concerns that various prewritten letters can address at different times in the communication.
- Scouting websites such as Craigslist in search of "wanted" advertisements and then contacting the advertisers as legitimate suppliers.
- Confidence, interpersonal persuasion, and misrepresentation: Subjects learn to confidently misrepresent themselves and others in online business transactions by learning how to communicate with

online buyers (what to say, how to say it, and how to address buyers' worries and win them over when they have doubts). To be convincing, subjects must sound knowledgeable of the merchandise they claim to supply and to provide justifications regarding why a buyer must make payment for the merchandise to Cameroon.

- Dealing with skeptical buyers: Buyers who are hard to convince are dealt with on a case-by-case basis. For example, some buyers can complain about a selling price being too high, while indicating their intentions to shop elsewhere. In such cases, subjects are taught to create a new account and contact that buyer with the knowledge they already have about the buyers' preferences. Time is important because scammers who take too long to scam a buyer run the risk of other scammers scamming the buyer first.
- Deceiving the same victim into making multiple payments by coming up with plausible stories about delivering merchandise, for example, money needed to insure the merchandise, pay for customs, or for quarantine. Importantly, learning how to do successful scams is a continuous process; subjects learned other important tactics to become a successful scammer, for example, how to avoid getting caught by law enforcement.

3.6.3.3 Stage 3: Justifying the Solution

Although becoming scammers was to address the problems outlined in Stage 1, movement into scamming did not make subjects immune from mainstream conventional culture. To cope with the moral and legal pain of committing the crime of scamming, subjects formulated justifications as defenses to their solution, that is, becoming Internet scammers.

A means to realize their long-term conventional goals

Because scamming is a crime and a moral vice, scammers justify their decisions to continue committing Internet scams by claiming that it is only a short-term means to achieve their long-term goals. Some scammers indicated that their long-term goals included traveling overseas; however, most indicated that they were already living these long-term goals, for example, enjoying their preferred lifestyle of fast money, girls, partying, and popularity. Most subjects, however, could not specify what their long-term goals were. Some subjects who were attending university indicated that scamming had made them drop-out of the university or at the very least, negatively affected their studies, for example, delaying their graduation from the university.

Love for the scammers' lifestyle

Subjects justify scamming for the extravagant lifestyle that includes reckless spending and being popular among friends, strangers, and girls. Scamming transformed them from ordinary individuals who were no different from the people in their neighborhoods to popular individuals who were known to

almost everyone. Furthermore, subjects indicated that they cannot do without this lifestyle.

Blaming others

The old generation subjects justified continuance in scamming by blaming the victims of scamming and the socioeconomic conditions of corruption and unemployment. Because their customers prefer unreasonably low selling prices and will quickly send the payment when a supplier agrees to a low price, the old generation subjects also mentioned this to justify continued scamming. Framing customers seeking the lowest possible price as greedy or dishonest enables subjects to claim that they are not the only ones involved in dishonest behaviors.

Effect of the harm from scamming

The new generation subjects defended their decisions to continue committing scams on the assumption that their victims are probably wealthy. Thus, they will not be too concerned about losing money from scamming. Subjects also suggested that some victims might not even realize that they have lost money. They reinforced this thesis by stating that they are only lower-level scammers, in contrast to their more successful peers committing "company scamming" (Subject 10).

Timing of their guilty feelings

Choosing scamming as a solution to their problems created feelings of guilt in some scammers, particularly the new generation subjects. However, they can cope with such guilty feelings because of the timing of the guilt. Subjects reported guilty feelings that are temporary and only emerge when they have successfully scammed a buyer. Subjects reported that their guilt is only after the act because of the reason for the act; that is, when they are planning and persuading buyers to make advance payments, they are overwhelmed by an urgent need for money to satisfy their extravagant lifestyles. Thus, they are not concerned about the effect of their actions on their victims. After a successful scam, however, these subjects experience guilt for several reasons:

- their continued attachment to the conventional norm through their relationships with God, upbringing, and socialization with their non-criminal friends;
- the guilt emerging from their consciences is beyond their control; and
- the post-scamming interactions some subjects have had with some of their victims.

Subjects described how some victims wrote to complain that they have been scammed and to explain why and for whom they needed the merchandise, for example, as a pet as present to a sick child or as a Christmas present. When subjects learned about these victims and their personal circumstances, they realized that some of their victims are "just like us." Despite the empathy they

felt, it was not strong enough to change their behaviors because of their own extravagant needs. In addition, subjects reported that, given the opportunity, they would say words of comfort that their victims want to hear to make the victims feel better. Such words of comfort also make subjects feel less guilty.

Karma

Although subjects indicated that scamming is wrong both legally and morally, they justified their continuance decision by suggesting that they were already paying the price for scamming through karma. Because of karma (what goes around comes around), subjects suggested that they cannot save enough money to meet their long-term goals and quit scamming. Hence, even though subjects view scamming to be wrong, they also claim that karma is one punishment for their crime.

Effectiveness of deterrence

Subjects also viewed scamming as the solution to their problems because they can evade justice while making fast money illegally. They suggested that the existing anti-scamming measures are ineffective and uncertain. Although law enforcement sometimes apprehends scammers operating out of cybercafés, they could not go after those operating with laptops from private locations, such as their homes. Subjects believe that operating from anywhere at any time makes it hard for law enforcement to track them.

Although local banks have instituted measures to curb scammers' activities, subjects reported finding successful ways to evade these measures. For example, when banks started blacklisting individuals suspected of scamming for three months, the blacklisted scammers hired pickups to collect the money on their behalf. Further, upon realizing that other scammers' collusions with law enforcement makes apprehension more likely, subjects reported that they stopped bragging about a successful scam until they collect the money from a financial institution.

When banks began proactively advising their customers against business deals with suppliers in some West African countries, subjects also advised them to lie about the nature of the transactions. When banks, acting as legal representatives of their customers, request documentation as proof that a supplier is legitimate, subjects reported obtaining the required documents from the Internet. Further, when Facebook changed its policy to reduce how many groups a Facebook user can join at a time, subjects settled for the reduced number of groups they could join. Even though subjects viewed this restriction as negatively affecting their scamming activities, they stated that they have adjusted well to it.

3.7 Discussion

3.7.1 Toward a stage theory

We develop an explanatory theory (Gregor, 2006) that explains how one becomes an Internet scammer. We theorize from our findings by proposing that becoming an Internet scammer unfolds in three stages, relating the findings to relevant extant literature and theory. Stage 1 focuses on the pre-scamming problems and negative emotions that motivated subjects' journeys into scamming and explains why they were motivated to become scammers. Stage 2 focuses on the learning process and why subjects chose to begin committing Internet scams. Stage 3 explains why they persist in Internet scamming. Further, we also relate our findings to relevant theories from criminology. Although the relevant crime theories (e.g., SLT and GST) are viewed as general theories of crime applicable to all forms of crime (proclivity toward crime and persistence in committing criminal acts), our overall finding suggests that no single previously developed dispositional and situational criminological theory can adequately explain how one becomes an Internet scammer.

3.7.1.1 Stage 1: Problems and Their Negative Emotions

Stage 1 addresses two problems. First, it explains why subjects made their first steps into scamming by agreeing to learn how to scam. Our finding differs from existing scamming research, which has suggested that the problems influencing people's decisions to become scammers are from preexisting socioeconomic conditions, such as poverty, corruption, and unemployment. Second, our Stage 1 finding also explains the role of money in becoming an Internet scammer. Although existing research has suggested that people are motivated by money to become scammers (Burrell, 2008; Abia et al., 2011), it has not explained why money is a motivator.

Subjects' decisions to learn how to scam were influenced by two problems, one for each generation of scammers. For the new generation, it was that friends became Internet scammers. This problem resulted in the negative emotional feeling of loneliness because their friends could no longer make time to socialize with them. The old generation's problem was loss of business income, and it resulted in the following negative emotions: anger, disillusionment, and revenge. These negative emotions emerged for two reasons: (1) some subjects viewed the problem as a threat to their financial independence and their abilities to sustain their families and (2) subjects blamed their problems on others, such as the government (its inability to manage corruption and reward meritorious hard work), greedy customers, and dishonest suppliers. Although the old generation subjects blamed the government for part of their problem, the finding suggests the main source of their problem is situated at the personal/business level.

Accordingly, we suggest that subjects' respective problems and the negative emotions they subsequently produced motivated their decisions to

learn how to scam for the following reasons: (1) Those whose friends became scammers socialized with scammers, personally experienced their lifestyle, and became attracted to the scammers' lifestyle of fast money and extravagance. (2) They also found the cost of the lifestyle to be too expensive to sustain without enough money. Consequently, they felt internally pressured and were externally pressured by their scammer friends to learn how to scam and keep up with the lifestyle. Additionally, (3) those whose businesses failed interpreted the loss of their business income as threats to their financial independence and their abilities to sustain their families. Thus, regarding the role of money, our finding suggests that money motivated subjects to become scammers because subjects needed the money to socialize and enjoy an extravagant lifestyle. Others additionally needed the money to maintain and protect their financial independence.

Relationship with existing literature and theory

Theoretically, the problems and negative emotions they produce can be understood through the lens of the GST and SLT. According to GST, negative emotions, such as anger, loneliness, or revenge, emerging from stressful events (e.g., inability to achieve monetary success, peer pressure, or death of a friend) increase the likelihood of crime. In particular, GST regards anger as the emotion that is most conducive to crime because it creates a strong desire for revenge and reduces the desire for legal coping. Crime, therefore, becomes an escape from the strain that produces these negative emotions.

Moreover, GST suggests the inability to cope as the main reason negative emotions from strains result in crime; our finding provides a more specific explanation, suggesting reasons subjects were unable to cope. For the old generation subjects, we suggest that the negative emotions (anger, revenge, and disillusionment) resulting from the strain, such as loss of business income, motivated subjects' decisions to progress into scamming because they wanted to protect their financial independence. In addition, they could not cope with the behaviors of their business partners (Subjects 1 and 2) and the corrupt political system.

For the new generation, we suggest that the desire to maintain friendships after friends became scammers was motivated by the need to protect themselves against loneliness. This was necessary because with scamming, their scammer friends had a new activity that they did not share with the subjects. In addition, because of scamming, their scammer friends had made new friends that they also did not have in common. After experiencing the extravagant lifestyle of scammers, it became a positive experience that they were unwilling to abandon. The lifestyle enabled them to hang out with their friends, make fast money, and become popular.

The importance of identifying the negative emotions that motivated subjects to learn to scam is that we not only understand the source of their problems, but we can also explain why they were unable to legally cope with their strains. These problems emerged from their personal and business activities and relationships at the individual level. Thus, even though subjects

indicated that they were affected by socioeconomic problems of poverty, unemployment, and corruption, the main source of the strains and negative emotions were within their personal control. We suggest that subjects blamed their problems on the macro system to invoke a narrative that misrepresents the problems as unjust, unavoidable, and beyond their control because the problems are caused by the socioeconomic environment. Further, invoking this new narrative made their decisions to learn how to scam appear reasonable. Indeed, when one considers the socioeconomic environment in Cameroon this narrative seems plausible.

Overall, therefore, Stage 1 findings focus on why Internet scammers made their first steps into scamming by identifying and explaining the source of their problems and the negative emotions the problems produced. In providing this explanation, Stage 1 also contributes to why subjects were motivated to learn to become scammers.

The Stage 1 finding is also related to the SLT. The SLT offers a general explanation of the acquisition, maintenance, and change in criminal behavior through associations with criminals (Akers et al., 2009). According to the SLT, criminal associations result in crime because they are of long duration, intimate, and occur frequently. Thus, a person does not become a criminal by merely associating with criminals; it is the nature, characteristics, and balance of the differential associations that affect a persons' likelihood of becoming a criminal (Akers & Jennings, 2009). The SLT, however, does not specify why criminal associations occur beyond that their occurrence is for criminal purposes. Similar to the SLT (Akers & Jennings, 2009), we find that scamming behavior is learned in a process of socialization with other scammers. Moreover, we also find that social learning leads people to scamming because of their desire to maintain and protect friendships, the love of the scammers' lifestyle, and their desire to become popular and respected among peers and to cope with peer pressure.

Whereas some individuals learned how to scam from close personal friends, others (e.g., the old generation scammers) learned individually by opportunistically observing other scammers and then by trial and error. This suggests that not all criminal learning emerges from personal socialization processes. Individuals overwhelmed by negative emotions (anger, revenge, and disillusionment) resulting from financial strains can become self-motivated to address these problems through criminal involvement. Overall, however, our finding highlights the important role that maintaining and protecting personal relationships and lifestyle preferences have in criminal associations. These relationships and preferences have not been reported in social learning and on previous empirical studies on SLT.

3.7.1.2 Stage 2: Solution: Learning and Committing Internet Scams

Choosing Internet scamming

Stage 2 explains why subjects chose scamming as the solution to their conventional problems. It starts by providing some context as to why scammers view scamming as a solution. That is, why the negative emotions from Stage 1

led subjects to conclude that conventional work does not pay and that it exposes one to disrespect and disappointment when the macro system is corrupt and does not reward merit. Consequently, we suggest that subjects specifically chose scamming and not some other crime (e.g., street burglary) for the following reasons:

- it is consistent with the subjects' preference for money, extravagance, and popularity;
- subjects' proximity to scammers, access to scammers, and socialization with scammers; and
- the scams are committed online and IT reduces the complexity of interactions with online buyers.

Examples of the third reason include using Facebook and other websites to advertise scams, when scammers rely on prewritten letters and online anonymity that presents opportunities to evade being identified and/or apprehended.

Relationship with theory

Regarding preferences, similar to the RCT (McCarthy, 2002), we find that one of the reasons subjects decided to become scammers is that it is consistent with their preferences for extravagance, fast money, and popularity. Although RCT provides an account of how people's decisions depend on their preferences, RCT takes preferences as given (Paternoster & Pogarsky, 2009). Thus, RCT does not explain the source of people's preferences (McCarthy, 2002). Yet, to be rational means to act in a way that is harmonious with one's choices or preferences (McCarthy, 2002). In the case of this study, the source of subjects' preferences is the problems identified in Stage 1. Theoretically, this is important because by suggesting that preferences are affected by stressful events in people's everyday lives and by their personal relationships, we highlight a relationship between RCT, GST, and SLT. However, because RCT does not explain the source of a preference, it cannot adequately explain why subjects' problems motivated their decisions to commit Internet scams.

3.7.1.3 Solution: Committing Internet scams

Our Stage 2 finding also explains why subjects chose to commit Internet scams after learning how the scams are committed. The main reason is that the scams are committed through a CMC medium. The act of committing Internet scams involves online persuasive misrepresentations. Internet scammers misrepresent themselves, organizations, persons, locations, merchandise, and offers. Our finding explains the role of learning and associations that detail what subjects learned and how the CMC medium facilitated their decisions to start committing Internet scamming. The technique of committing persuasion by misrepresentation is to deceive online consumers into making advance payments for nonexistent merchandise. Learning to perpetrate these misrepresentations requires socialization with Internet scammers.

To successfully commit Internet scams, subjects learned two techniques of misrepresentations, namely, IT-enabled misrepresentations and IT-facilitated misrepresentations. Both techniques and their characteristics are shown in Table 5.

TABLE 5 Types of IT-misrepresentations

IT-enabled misrepresentation technique	**IT-facilitated** misrepresentations
Displaying false geographical locations, assuming multiple genders/identities, posting nonexistent merchandise on websites and on Facebook, and operating from anywhere and at any time of the day	Internet technology as a platform to perform social persuasive communication: credibility by pretending to have expertise and knowledge about a merchandise displaying false empathy, enabling them to deceive an online buyer of merchandise or an online seeker of a romantic relationship.

In addition, IT-enabled misrepresentations are those behaviors that have emerged and are practicable because of Internet communications (e.g., displaying multiple identities). Indeed, the attributes of IT-enabled misrepresentation have been mentioned in headline news and the research literature on scamming (e.g., Burrell, 2008). However, past scamming research does not differentiate between IT-enabled and IT-facilitated misrepresentations. The IT-facilitated misrepresentations (e.g., displaying false empathy) involve using Internet technology as a platform to perform persuasive social communication. The online context in which Internet scammers operate enables them to apply social influence techniques in ways they might not be able to in the physical world. Although both social learning and differential association theories describe the importance of learning specific techniques of committing a crime, neither theory specifies a particular technique. This is because the learning theories of crime were developed as general theories, applicable to all forms of criminal acts.

We specify the tactics that scammers use to commit scams and, in doing so, highlight the important role that information technology through certain Internet attributes plays in the commission of Internet scams. Further, we explain that individuals who learn to commit scams take the next step to execute what they have learned as Internet scammers because the scams are committed through the Internet. This finding provides a more specific explanation for the generic one in SLT. According to social learning, people commit crimes when they develop definitions that are favorable to violations of the law in excess of definitions favorable to conformity. Our finding, moreover, specifies that, in the context of Internet scamming, the Internet represents a key definition favorable to violation of the law.

First, regarding the specific tactics used by scammers, we suggest that addressing this problem requires considering the two features of IT-enabled and IT-facilitated misrepresentations. Both techniques give scammers the

confidence to commit Internet scams while also bringing them closer to their victims. In addition, the Internet enables them to appear credible and legitimate by filtering out undesirable social cues (e.g., location, physical appearance, race, or gender). Consequently, Internet scammers are freed from the relevant physical constraints of time, place, race, and sanctions. Figure 2 (in Appendix 2) shows how the Internet enables these online misrepresentations.

Further, subjects' decisions to start committing Internet scams were also affected by what they learned about the tricks of committing an Internet scam. These include utilizing Facebook as the main medium for finding, communicating, and deceiving online users because it enables live chats and reduces the time to response in comparison to email communications. Moreover, they use prewritten letters to reduce mistakes and utilize anonymity as a veil to hide deceptive cues (e.g., location, gender, race, or age) and to communicate confidence and persuasion. Through CMC, subjects can approach the same victims under different user names and deceive them multiple times. Further, these characteristics of Internet technology highlight key differences between physical crimes (e.g., face-to-face scams) and scamming on the Internet. Theoretically, these differences highlight a need for understanding online crimes as distinct from offline crimes.

Furthermore, Stage 3 explains why Internet scammers persist in scamming. The findings highlight the combined roles of deterrence ineffectiveness, anonymity, scammers' subjective thinking processes, and justifications for persisting in scamming.

3.7.1.4 Why deterrence is ineffective?

Overall, our finding identifies several reasons deterrence is ineffective, which are discussed below. These include Internet anonymity, pickups, and scammers' subjective thinking assessment processes. According to deterrence theory, the deterrence effect is assumed to deter offenders and would-be offenders from engaging in crime. However, the empirical evidence is also inconclusive, contested, and dependent on the specific crime (Tonry, 2008; Naggin, 1998). Criminologists suggest that an effective deterrence measure should be based on the specific form of the crime, how it is perpetrated, the process by which people learn to commit the crime, and how offenders perceive the deterrence measures. This suggests a bias toward studies with fine-grained details. While such details provide relevant knowledge for policymakers, deterrence measures that fail to consider offenders' views can lead to the adoption of mistaken policies (Tonry, 2008). In the next section, we explain why deterrence against scamming is ineffective from the perspective of Internet scammers.

Internet anonymity and pickups

First, subjects view deterrence as ineffective because of Internet anonymity, which acts as a veil to hide them from their victims and law enforcement. Anonymity obscures their identities and ensures that they appear credible and believable to online buyers. This cloak of anonymity, however, is not always

anonymous. When scammers successfully persuade a buyer to make advance payments, they must send buyers their real identities for the money to be transferred. Thus, anonymity is salient up until the point that Internet scammers need to receive an advance payment. However, scammers can hire the services of a pickup to preserve their anonymity and protect themselves against the risks of being caught in the process of collecting the scamming money. Further, the availability of pickups strengthens scammers' perception that deterrence measures are ineffective.

Subjective thinking processes

Second, deterrence is also ineffective because of scammers' subjective thinking toward deterrence measures. By subjective thinking, we mean how scammers assess deterrence measures. They assess the measures through factual and biased information.

The assessment, based on factual information comes from their experiences operating as Internet scammers. It leads scammers to consider the severity, certainty, and celerity of anti-scamming measures in line with the expectations of policymakers. However, the particularity of the local context exposes scammers to ways to avoid deterrence measures, for example, giving bribes, using pickups, and avoiding cybercafés. Consequently, they have come to view deterrence implementation as uncertain and sanctions as avoidable. In contrast, scammers view the collusions between other scammers and law enforcement as the most effective means of apprehension. Because scammers view bragging as the source of this problem, they avoid bragging about a successful scam.

Offenders' biased subjective thinking process

In contrast, Internet scammers' deterrence assessment based on biased information is influenced by their wishful thinking. This includes their hopes and personal expectations, and the limited and/or distorted information they are aware of about anonymity and anti-scamming deterrence measures. These biases stem from scammers' specific and general knowledge that the implementation of anti-scamming measures is uncertain. However, their knowledge is also limited to only those deterrence measures that they have experienced. Nonetheless, the uncertainty of implementing deterrence and a lack of visibility of law enforcement, leads Internet scammers to conclude that anti-scamming measures are either ineffective or nonexistent.

Further, their wishful thinking bias leads scammers to conclude that information technology in Cameroon is so porous and underdeveloped that they cannot be tracked while using laptops from private locations to commit scams. Here, scammers' factual subjective assessment is that information technology in the Cameroonian and West African context is underdeveloped. However, their interpretation that the systems to track online criminals are nonexistent, ineffective, corrupt, or too costly to be deployed is biased because it is not based on accurate information. Importantly, these biased views enable a conclusion in scammers' favor about the uncertainty of getting caught while

practicing Internet scams. In addition, their views that sanctions become ineffective when they no longer operate from cybercafés are also biased because it undermines the fact that most individuals can be tracked through their Internet IP addresses. The same is true for those scammers who said they were "low-level scammers" and thus concluded that the cost to international agencies of apprehending low-level scammers outweighs the money lost by their victims.

Overall, the subjective thinking is biased for these reasons. First, it is based on limited information. Internet scammers lack reliable information about the "behind the scenes" efforts and the progress that is being made toward apprehending them. Second, it is based on wishful thinking. Internet scammers want to belief that deterrence does not work and hope that they will not be apprehended. Therefore, even though Internet scammers are influenced by both factual and biased thinking processes, they give more weight to their biased understanding. Importantly, their biased understanding influences their decisions not to quit scamming. They are influenced by the uncertainty of sanctions and the low cost of scamming. From our finding, we approximated subjects' factual and biased subjective assessment processes in Table 6.

TABLE 6 Subjects' factual and biased subjective assessment processes of deterrence countermeasures

Threat or certainty of sanctions is reduced by a combination of	Threat or certainty of sanctions is increased by a combination of
distance from victims + use of personal laptops + poor IT infrastructure + police corruption + corrupt bank tellers + pickups + fewer postings + short/long-term goals + monetary benefits + lifestyle	collusion between jealous internet scammers and police officers + restrictions on posting of adverts on Facebook + user awareness

Use of justification

Subjects also misrepresent the problems in the social structure (e.g., unemployment and corruption), engage in "therapy sessions" with victims, and use self-deception to justify continuing to commit Internet scamming. They misrepresent preexisting problems in the sociopolitical system by claiming that everyone is corrupt and condemning anyone who condemns them. Specifically, the old generation scammers deny responsibility for scamming by claiming that they have tried and failed to manage conventional businesses because the system does not reward merit. They engage in "therapy sessions" with victims to alleviate their guilty consciences, for example, saying "sorry" to a victim is often a pretentious display of empathy. However, they noted that their remorse is sometimes genuine. Such remorse is also an indication of subjects' continued commitment to conventional values. Thus, Internet scammers' expressions of remorse serve two purposes: temporarily relieving them from their guilty consciences and helping their victims to feel better. Further, subjects rely on

self-deception to persist in scamming. Self-deception involves scammers lying to themselves about quitting. For example, the new generation scammers claim that scamming is only a short-term activity and that they will quit once they have saved enough money to start a conventional business or travel overseas. However, they also justify continuing by blaming karma and their extravagant lifestyles as preventing them from saving money.

A final reason for persisting is the timing and duration of their moral guilt. Subjects who reported guilt tend to only experience the guilt after a successful scam. Their preference for the lifestyle of extravagance, popularity, and fast money affects the timing of any remorse they may feel because the lifestyle is more important and rewarding than forgiveness. Thus, when subjects use up all their money and feel the urgency to scam, remorse disappears.

Relationship with theory

In the IS security literature, the use of neutralization has been associated with (1) reducing the deterrence effect of sanctions (Siponen & Vance, 2010), (2) convenience (Barlow et al., 2013), and (3) completing a task (Puhakainen & Ahonen, 2006). Internet scammers, however, invoke neutralizations to justify continuing in crime. This study, therefore, provides views on the most common justifications used by scammers who want to persist in the crime of Internet scamming. Our findings suggest that Internet scammers use neutralization techniques to justify continuing in scamming in the following ways: condemning those who condemn or are likely to condemn their actions as wrong, for example, society, church leaders, or the government; denying responsibility for their actions by pointing to their failed attempts do conventional activities; invoking karma to suggest that they too are victims; and displaying empathy for their victims to claim that they mean no harm. The way scammers use neutralization to justify their behaviors suggests that its use is specific to the type of crime or violation. The justifications we have identified as being used by scammers can be incorporated in anti-scamming programs. However, IS researchers have also called on researchers to explain the reasons people use neutralizations (Siponen & Vance, 2010). We suggest that Internet scammers use neutralization to highlight the problems and the negative emotions they experienced before they became scammers and to protect their choice of scamming as their solution to these problems. This further highlights why, in the scamming context, neutralization is more suited to explaining why Internet scammers persist in scamming than why they became scammers.

3.7.2 Contributions

Even though scamming has become a major form of cybercrime, to date, research on scamming has primarily focused on why people become scammers. Extant scamming research suggests that money, structural problems, and Internet access are the main reasons people become scammers. We argue that, while the existing explanations are plausible, they do not tell the whole story. Therefore, we explain why the factors identified in previous research (money,

structural problems, and Internet access) motivate people to become scammers. Moreover, extant research does not explain how one becomes an Internet scammer. This is important because addressing the scamming problem should preferably rely on interventions that are effective at the earliest possible stage. Therefore, we propose a theory with three stages that shows how individuals progress into scamming and persisting in scamming. Each stage focuses on a different problem. Theoretically, our stage-based explanations suggest that no single dispositional and situational criminological theory can adequately explain the phenomena of becoming an Internet scammer and persisting as one. Instead, aspects of different criminological theories are relevant at different stages regarding how one becomes an Internet scammer.

Stage 1 focuses on why individuals make the first steps toward scamming by agreeing to learn and to start committing Internet scams. In other words, Stage 1 explains why one becomes an Internet scammer. Past research suggests that people are motivated by money, structural problems, and access to the Internet to become scammers. Our research goes further and explains why these factors motivate individuals to become scammers. These issues are not addressed in the extant scamming literature. We suggest that money motivates individuals because it is needed to socialize, to enjoy an extravagant lifestyle, and to become financially independent. Money is therefore a means for scammers to cope with the negative emotions (loneliness, anger, revenge, and disillusionment) from the problems arising from their pre-scamming activities and relationships. We further contribute to why people become scammers through the question: *Where do the problems that propel individuals into scamming originate?* Because past scamming research has suggested that the problems that lead people toward scamming are preexisting in the socioeconomic environment, researchers and commentators have called for sociopolitical changes in the West African countries most affected by scammers' activities (Burrell, 2008; Peele, 2005). In contrast, we identify and situate the source of scammers' problems as mainly personal, from their activities and relationships. We suggest that when scammers were unable to cope with their personal problems, they invoked a narrative that misrepresented the problems as unjust, unavoidable, and beyond their control to blame these problems on the preexisting structural problems, such as poverty, unemployment, and corruption (Akinladejo, 2007; Atta-Asamoah, 2009; Burrell, 2008). Therefore, whereas the scamming literature traces the source of the problem at the structural level, our finding traces the main source of their problems at the individual level.

Theoretically, the identified pre-scamming individual problems (friends became Internet scammers and loss of business income) and the respective negative emotions they produced (i.e., loneliness for the former and revenge, anger, and disillusionment for the latter) can be explained through GST and SLT. Whereas GST suggests that individuals become involved in crime because they are unable to cope with the negative emotions from their strains, our contribution explains why they are unable to cope. For some individuals, a

strain (e.g., loss of business income) and the negative emotions it produces (anger, revenge, and disillusionment) lead to crime because they are determined to maintain and protect their financial independence. For others, a strain (e.g., friends became Internet scammers) and the negative emotion it produces (loneliness) will lead to crime because these individuals have been exposed to the lifestyle of scammers, love the lifestyle, and cannot sustain the cost of the lifestyle without becoming scammers themselves. With regards to SLT, although it was developed to explain why socialization with criminals could lead to crime, SLT does not specify the source of criminal associations except that such associations often lead to crime. Our contribution to SLT, therefore explains why subjects associated with other scammers before they became scammers and improves our understanding of the socialization processes that result in Internet scamming. Associations with scammers occur and lead to crime because of an individuals' desire to maintain and protect their friendships, the love of the lifestyle, the respect among peers, and the peer pressure and because such associations reinforce their preexisting views that conventional work exposes one to disrespect and disappointment in a corrupt system that does not reward merit. The SLT lacks such specificity because it was developed as a general theory, applicable to any form of crime.

The contribution in Stage 2 focuses on why individuals specifically commit Internet scams and not, for example, street robbery or burglary. We identified the following reasons for this. First, scamming is consistent with these individuals' preferences. Traditionally, preferences are associated with RCT. Rationality refers to people acting in ways that are consistent with their preferences (McCarthy, 2002). First, similar to RCT, we find that individuals commit Internet scams because it is consistent with their preferences for fast money, popularity, socialization with friends, financial independence, and extravagance. However, because RCT takes preferences as given, it does not explain the source or origins of a preference. Therefore, RCT cannot adequately explain why a preference will motivate one to commit a crime. We suggest that, in addition to time discounting, costs, and benefits, preferences are also affected by historical problems, associations, and the ensuing emotions. These additions from our findings suggest a consistent relationship between RCT (preferences), GST (problems and emotions), and SLT (associations) in the decision to commit a particular crime. Researchers have argued that because RCT takes the source of preferences for granted, it is incompatible with theories that argue that structural conditions or socialization processes affect a disposition to commit crime (e.g., (e.g., Gottfredson & Hirschi, 1990; Herrnstein & Wilson, 1985).

Our second contribution in Stage 2 identifies the Internet and its capability to reduce the complexity of social interactions as a reason individuals commit Internet scams. Because of the Internet's computer-mediated channel, individuals can commit scams through two forms of misrepresentations: IT-enabled misrepresentations and IT-facilitated misrepresentations. The relationship between the two forms of misrepresentations is interdependent. Although IT-enabled misrepresentations (e.g., possessing multiple identities,

locations, genders, or races) have been mentioned in the scamming literature (Burrell, 2008), they have not been distinguished from IT-facilitated misrepresentations, which are persuasive skills that can be performed in a physical setting but are enhanced in an online setting. We suggest that both techniques enable individuals to commit scams and enhance the success likelihood of a scam by giving and/or improving scammers' user attributes (confidence, legitimacy, authority, and authenticity), filtering out socially undesirable attributes (e.g., location), and freeing scammers from physical constraints (e.g., time, place, or race). Identifying the specific socialization processes of committing a scam also contributes to SLT. Although the principles of SLT highlight an important role for socialization in the criminal process, SLT does not specify the techniques and means of committing any particular crime (Akers & Jennings, 2009). Further, identifying the specific contents of IT-enabled and IT-facilitated misrepresentations, our findings underscore how committing scams online differs from committing scams and other crimes (e.g., robbery) offline. This also highlights the need to study crimes committed in cyberspace as distinct from crimes committed in the physical environment.

Our Stage 3 contributes to determining why Internet scammers persist in scamming; that is, their continuance behavior. Our first contribution on this relates to deterrence: Why is deterrence against scammers ineffective? We find that existing measures neither consider the views from the offenders (scammers) nor the particularity of the local contexts from which scammers operate. Criminologists suggest the reason deterrence results are often inconclusive and contested is that they are based on macro-level data that do not consider fine-grained details, such as the specific form of the crime, the means by which it is perpetrated, the process by which people learn to commit the crime, and how offenders perceive the deterrence measures (Nagin, 1998; Tonry, 2008).

In the scamming context, deterrence is ineffective for the following reasons:

- scammers rely on Internet anonymity to obscure their identities, assume false identities, and hide from law enforcement;
- scammers can hire the services of a pickup who will assume the risks of getting caught or blacklisted;
- scammers can convince their victims to lie about what the money is for and fabricate false documentation if the need arises; and
- scammers assess deterrence through two subjective thinking processes (i.e., factual and biased).

Although the factual thinking process includes the deterrence effect (severity, certainty, and celerity of sanctions), its effect is seriously reduced by the particularity of the local context that exposes scammers to ways of avoiding the deterrence effect, for example, giving bribes, using pickups, avoiding bragging, and avoiding using cybercafés. Consequently, the locale makes scammers view the deterrence effect as uncertain and avoidable. Thus, relying

on context-specific evidence, we explain why the deterrence effect is ineffective. In doing so, we highlight a relationship between deterrence and anonymity from the offender's perspective.

Researchers in criminology (Gibbs, 1975) and IS security (Willison & Warkentin, 2013) have called for offenders' subjective thinking to be empirically examined. Relying on secondary data, the scamming literature recommends very severe punishment for scamming (Akinladejo, 2007). Our evidence, however, suggests this is not effective. In the IS security literature, because security policies do not necessarily deter IS misuse behaviors, researchers have speculated that, as users become more aware of security policies, they may realize that detecting IS misuse behavior is fraught with difficulties (D'Arcy, Hovav, & Galletta, 2009c). Our evidence suggests that a major problem for deterrence countermeasures and policymakers is offenders' subjective assessments of the countermeasures.

3.7.3 Implications for Practice

There are several anti-scamming recommendations in research and practitioner publications. Our evidence from scammers suggests their effectiveness is questionable. Examples of existing recommendations include appeals for policymakers, governments, and international organizations to unite in the fight against scamming (Salifu, 2008), closing cybercafés and websites used by scammers (Abia et al., 2010), deleting profiles that are associated with scammers' activities (Rege, 2009), and severe sanctions against scammers (Salifu, 2008). A major reason is that the extant recommendations are based on secondary data. Thus, they are not based on clearly identified and understood problems. Our recommendations, while primarily relevant to a particular context, can be adjusted to suit the problems of scammers in other contexts. The context from this study includes an environment rife with structural problems, such as poverty, unemployment, and porous technological infrastructure.

Overall, our findings and analysis led us to recommend that interventions against scamming should begin by identifying and conversing with key stakeholders. This will lead law enforcement to identify the problems associated with becoming a scammer in a particular locale. This approach ensures that anti-scamming measures are not based on out-of-context external views.

Specifically, focusing on the problems identified in this study, we identify three categories of individuals that should be the focus of anti-scamming interventions, namely, teenage scammers (e.g., new generation scammers), more experienced scammers (e.g., old generation scammers), and would-be scammers (including pickups). Achieving the goal of changing the behaviors of these categories of individuals by discouraging them from becoming scammers (would-be scammers) or from continuing scamming (new and old generation scammers) should begin by assessing what their respective problems are and how they need to change.

Internet scammers (new and old generations) complain that the problem is multi-level (individual and socioeconomic); however, our evidence suggests that personal and business problems, love of an extravagant lifestyle, and protection of their financial independence motivated their decisions to become scammers. We recommend that intervention programs emphasize this lifestyle preference in anti-scamming messages. We also recommend they approach appeals to poverty, unemployment, or corruption as justifications. They should also emphasize that those scammers with no work-related skills will not be qualified for any conventional work anyway. The long-term consequences of sanctions, for example, having one's name blacklisted online forever, should also be emphasized. The anti-scamming message should also be uplifting, motivating scammers to feel less fearful of the consequences of quitting and leaving behind the lifestyle of scammers. Particularly, the new generation scammers should be encouraged to return to school, complete their degrees, or learn a new trade.

On one hand, we recommend that anti-scamming messages be broadcast through radio and television channels. This will ensure the messages reach a wider pool of stakeholders than just the offending scammers, for example, parents, church and community leaders, would-be scammers, and teachers. Parents, teachers, and church leaders are important stakeholders that are currently ignored in the fight against scamming. The importance of reaching parents through a formal channel is that they can also discipline and/or advise their children who are scammers to quit. In addition, it is also expected that parents will advise their children (would-be scammers) against associating with friends who are scammers. Parents of scammers can reinforce messages about the threat of prison time and blacklisting. A current policy by local banks to blacklist individuals suspected of engaging in Internet scamming for three months should be extended and publicized. While such measures will force Internet scammers to rely more on pickups, we are hopeful they will instill a fear in would-be scammers and pickups that crime is futile.

While teachers can play the same role in schools, a much more effective approach would be to include cybercrime in school's guidance and orientation programs. Guidance counselors in schools should be trained to talk about the risks of cybercrimes, such as scamming. As an increasing number of teenagers are following their friends into scamming, national and international organizations that fight scamming should direct their focus to schools targeting would-be scammers and the new generation scammers. In addition, the messages should also emphasize self-esteem and confidence against the temptation to make fast money. Scammers and would-be scammers should be encouraged to change their behaviors or focus from immediate gratification to long-term gratification, for example, through education or vocational programs. Although it might seem obvious, most Internet scammers and those at risk of becoming scammers are not aware of these long-term consequences. The messages should also emphasize that anonymity is overrated and

improvements in digital technology mean that Internet criminals are more likely to be tracked and apprehended.

Another approach can involve approaching neighborhood organizations and finding key informants who have access to scammers. Neighborhood groups already exist in most local communities across West Africa; importantly, targeting neighborhood meetings means targeting parents of scammers, would-be scammers, and pickups. The goal would be to get scammers to talk about their problems to specially trained social workers who can also advise based on each scammer's individual circumstances. This approach will more likely be successful if spearheaded and sponsored by collaboration between the national governments and international organizations, particularly crime agencies that have so far mainly focused on sanctions. Well-publicized crackdowns should be carried out occasionally to instill fear and challenge the prevailing biases in the scamming community that deterrence is not enforced and that it is ineffective when enforced.

3.7.4 Study Limitations and Directions for Future Research

Like most empirical studies, this study has limitations that should be acknowledged. First, this study did not actively focus on the neighborhoods of scammers and whether certain neighborhoods are producing more scammers. We did, however, observe that the cybercafés in certain neighborhoods were hotspots for would-be scammers. Efforts to reduce Internet scams would benefit from the additional explanations that a study of these neighborhoods could offer.

Our study focused on "black-hat" cybercriminals. We have also relied on data from these criminals to recommend interventions targeting youths at risk of becoming Internet scammers. However, a much better approach might involve studying the individuals who have desisted from scamming, that is, former Internet scammers. The findings, on one hand, will also contribute to programs dedicated to preventing people from becoming Internet scammers. On the other hand, they will contribute to programs aimed at motivating practicing Internet scammers to quit. Second, because becoming an Internet scammer is a continuous learning process, future research can adopt a longitudinal lens in which the scammers are studied throughout the learning process. The finding will particularly contribute to IS security research and SLT.

Further, the effectiveness of scam-baiting should be empirically studied. Scam baiters argue that by wasting scammers' time, they are effectively contributing to protecting some online consumers. Given the number of Internet scammers, it might also be that scam-baiting takes more time and effort (e.g., setting up fake banks, user profiles, chatting with scammers) than the results it produces. Further, if scam-baiting were successful, it is likely that national and international crime agencies (e.g., the FBI) and technology companies, such as Facebook, would start producing software that would automatically bait scammers to waste their time. However, despite the claims by scam baiters about their effectiveness, no empirical evidence exists to

suggest they are an effective deterrent. Future research can examine this dilemma.

Although it seems plausible that strained individuals who commit crime will use one or many techniques of neutralization, the relationship between neutralization and strain-induced crime has not been empirically examined. Although several empirical studies on strain and crime exist in the criminology literature, security researchers could further examine the mediator role of neutralization in the relationship between strain and cybercrime or other forms of IS violations. The findings would not only explain how individuals (organizational employees or cybercriminals) abuse a strain experience to commit a security violation, it would additionally explain neutralization through a new theoretical lens. Further, other equally important strains could be identified as a result of scammers operating in different regions of the world and their relationships with cybercrime (e.g., through neutralization) could be further explored.

3.8 Conclusion

Internet scammers pose a major problem for online consumers and ecommerce; they swindle people into giving up their money as advance payments for nonexistent merchandise. Despite the problems posed by Internet scammers, the scamming literature is hindered by problems, such as lack of authentic data and limited samples. The explanations offered by extant scamming studies regarding why people become Internet scammers include monetary reward, access to Internet in poor communities, and structural problems of poverty, corruption, and unemployment. Though plausible, we have argued that these explanations do not tell the whole story regarding why one becomes an Internet scammer; moreover, they do not explain how one becomes an Internet scammer.

We have addressed these problems by interviewing actual Internet scammers. Prior research has only suggested that money explains why people become scammers. Our finding, moreover, explains why money motivates individuals to become scammers. We reported that money is needed to socialize, to enjoy the extravagant lifestyle of scammers, and to become financially independent. While this contribution focuses on why individuals become Internet scammers, we also explain how individuals become scammers. Our findings identified three stages. Stage 1 explains scammers' pre-scamming activities and relationships resulting in problems and negative emotions that motivate their first steps toward scamming. Stage 2 explains why individuals specifically become scammers through their associations, lifestyle preferences, and desires to maintain financial independence. Stage 3 explains why scammers persist in scamming through justifications, deterrence, and using pickups. We analyzed these findings regarding relevant dispositional and situational crime theories. First, we suggest that none of the extant dispositional crime theories

that explain proclivity toward criminality (e.g., SLT), can adequately and specifically explain why people become scammers. This is because becoming a scammer is affected by a combination of individual preferences, prior personal events and relationships, specific strains, and the negative emotions they produce. We also suggested that, although situational crime theories (e.g., RAT) were developed to explain why criminal acts occur, they cannot adequately explain why scamming occurs because they can neither explain the role of the offender nor the role of the computer-mediated environment in criminality. Thus, we highlighted the need for context-specific theorizing to explain Internet crimes, such as scamming. We further explain how such theorizing has implications for practice regarding combating Internet scams, for example, understanding the locales scammers operate from, how scammers subjectively assess deterrence, and why they use justifications and pickups before developing anti-scamming interventions. Further, the interventions should include a combination of education, fear, and sanctions, targeting not only practicing scammers but also would-be scammers.

4 OVERALL CONCLUSION

The Internet has evolved into a complex, dynamic, and globally interconnected digital and information infrastructure. Its ubiquity has made online behaviors, such as ecommerce, communicating (e.g., via email, instant messaging, and social media), and Internet browsing part of people's daily routines. Consequently, the Internet has become a minefield for of crimes, perpetuated on a global scale. This dissertation has addressed two types of Internet crimes from two perspectives: (1) phishing from the victims' perspective and (2) Internet scamming from the offenders' perspective. Whereas represents a major form of online identity theft, and Internet scamming is a major problem for ecommerce.

First, this dissertation examined how dispositional differences affect people's reasons for complying with phishing emails. This is based on the assumption in past phishing research that people are deceived by phishing emails for the same reasons. For example, past research considers that prior security experiences and online behaviors lead people to comply to threatening phishing emails for the same reasons. We argued that, although the act of clicking on a phishing link is the same for all phishing victims, the reasons for clicking will be different because they are affected by individual attributes, such as online behaviors, prior security knowledge, and experiences that affect people's behaviors in different ways. Adopting an inductive, grounded theory approach and relying on interviews with actual victims of phishing emails, this study examined the following the research question: How do differences in people's Internet behaviors affect their reasons for complying with phishing emails? Our contribution showed that the differences resulting from dispositional attributes (individuals' online behaviors and experiences) affect how they process and comply with phishing emails differently. Consequently, we theorized that phishing victims reside in one of two stages. Residence at a particular stage is affected by the differences stemming from how they process phishing. The phishing process attributes included: the nature of email and Internet use, prior security encounters, information security and privacy concerns, and encounters with phishing email. For practice, these differences

mean that anti-phishing recommendations should be tailored for different Internet users based on their stage of experience, knowledge, and online behaviors.

Second, this dissertation examined Internet scamming from the offenders' perspective. The question addressed was: how does one become an Internet scammer? We argued that, despite scamming research is at an exploratory stage, and only one study provided evidence from Internet scammers. Focusing on why people become scammers, past scamming findings suggested that people are motivated by (1) monetary rewards, (2) disillusionment with socioeconomic and political problems (corruption, unemployment, and poverty), and (3) affordable access to the Internet. We argued, however, that people motivated by monetary rewards, experiencing the above-mentioned problems, and are enjoying affordable access to the Internet do not become scammers. First, our empirical findings contributed to determining why people become scammers by explaining why money is a motivator. We reported that money is needed to socialize, to enjoy an extravagant lifestyle, and to become financially independent.

Second, we contributed to determining how individuals become scammers by identifying three stages. Stage 1 contributed to determining pre-scamming activities and relationships that produce negative emotions that motivate individuals toward scamming. Stage 2 contributed to determining specifically why individuals become scammers through their associations, lifestyle preferences, and desires to maintain financial independence. Stage 3 explains why scammers use neutralizations, deterrence, and rely on third parties (pickups) to justify persisting as Internet scammers. We analyzed these findings by relating them to theories in criminology. We reported that none of the extant dispositional crime theories that explain proclivity toward criminality (e.g., social learning theory) can adequately explain why people become scammers. We also reported that, although situational crime theories (e.g., routine activities theory) were developed to explain why criminal acts occur, they cannot adequately explain why scamming occurs because they can neither explain the role of the offender nor the role of the computer-mediated environment in criminality. For practice, we propose that interventions will be more effective when they consider the locales that scammers operate from and the scammers' subjective assessments of deterrence and emphasize education and fear for scammers and would-be scammers.

REFERENCES

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker Jr, J. F. (2010). Detecting fake websites: The contribution of statistical learning theory. *Mis Quarterly*, , 435-461.

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

Afroz, S., & Greenstadt, R. (2011). Phishzoo: Detecting phishing websites by looking at them. *Semantic Computing (ICSC), 2011 Fifth IEEE International Conference On,* 368-375.

Agnew, R. (1985). A revised strain theory of delinquency. *Social Forces, 64*(1), 151-167.

Agnew, R. (2001). Building on the foundation of general strain theory: Specifying the types of strain most likely to lead to crime and delinquency. *Journal of Research in Crime and Delinquency, 38*(4), 319-361.

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

Akinladejo, O. H. (2007). Advance fee fraud: Trends and issues in the caribbean. *Journal of Financial Crime, 14*(3), 320-339.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*, 69-82.

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), 67-79.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly, 34*(3), 613-643.

Atkinson, R., & Flint, J. (2004). Snowball sampling.

Atta-Asamoah, A. (2009). Understanding the west african cyber crime process. *African Security Studies, 18*(4), 105-114.

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

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! discouraging neutralization to reduce IT policy violation. *Computers & Security, 39*, 145-159.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1042.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3), 245-270.

Boateng, R., Olumide, L., Isabalija, R. S., & Budu, J. (2011). Sakawa–cybercrime and criminality in ghana. *Journal of Information Technology Impact, 11*(2), 85-100.

Brantingham, P. L., & Brantingham, P. J. (1975). Residential burglary and urban form. *Urban Studies, 12*(3), 273-284.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Broidy, L. M. (2001). A test of general strain theory. *Criminology, 39*(1), 9-36.

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)

Cacioppo, J. T., Petty, R. E., Kao, C. F., & Rodriguez, R. (1986). Central and peripheral routes to persuasion: An individual difference perspective. *Journal of Personality and Social Psychology, 51*(5), 1032.

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

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39*, 447-459.

Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice,* , 225-256.

Clarke, R. (1978). Tackling vandalism. home office research study no. 47.

Cohen, A. K. (1955). Delinquent boys; the culture of the gang.

Conklin, J. (2013). *Criminology* (11th ed.) Pearson.

Cornish, D., & Clarke, R. (1986). Rational choice approaches to crime. *The Reasoning Criminal: Rational Choice Perspectives on Offending,* , 1-6.

Cowan, D. A. (1986). Developing a process model of problem recognition. *Academy of Management Review, 11*(4), 763-776.

Crain, W. (2015). *Theories of development: Concepts and applications* Psychology Press.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643-658.

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

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

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

Das, E. H., de Wit, J. B., & Stroebe, W. (2003). Fear appeals motivate acceptance of action recommendations: Evidence for a positive bias in the processing of persuasive messages. *Personality & Social Psychology Bulletin, 29*(5), 650-664. doi:10.1177/0146167203029005009 [doi]

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior, 26*(6), 1739-1747.

Decker, S. H., Pyrooz, D. C., Sweeten, G., & Moule Jr, R. K. (2014). Validating self-nomination in gang research: Assessing differences in gang embeddedness across non-, current, and former gang members. *Journal of Quantitative Criminology, 30*(4), 577-598.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413-422.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the Second Symposium on Usable Privacy and Security,* 79-90.

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

Eide, E., Aasness, J., & Skjerpen, T. (1994). *Economics of crime: Deterrence and the rational offender* North-Holland.

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

Eitle, D. J. (2002). Exploring a source of deviance-producing strain for females: Perceived discrimination and general strain theory. *Journal of Criminal Justice, 30*(5), 429-442.

Eitle, D., & Turner, R. J. (2003). Stress exposure, race, and young adult male crime. *The Sociological Quarterly, 44*(2), 243-269.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence* Elsevier New York.

Glaser, B. G. (1978). *Theoretical sensitivity: Advances in the methodology of grounded theory* Sociology Press Mill Valley, CA.

Glickman, H. (2005). The nigerian "419" advance fee scams: Prank or peril? *Canadian Journal of African Studies/La Revue Canadienne Des Études Africaines, 39*(3), 460-489.

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

Grasmick, H. G., & Bursik Jr, R. J. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. *Law and Society Review,* , 837-861.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly,* , 257-278.

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review, 40*(2), 265-281.

Hay, C., & Evans, M. M. (2006). Violent victimization and involvement in delinquency: Examining predictions from general strain theory. *Journal of Criminal Justice, 34*(3), 261-274.

Hekkala, R., & Urquhart, C. (2013). Everyday power struggles: Living in an IOIS project. *European Journal of Information Systems, 22*(1), 76-94.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Herley, C. (2012). Why do nigerian scammers say they are from nigeria? *Weis,*

Herrnstein, R., & Wilson, J. Q. (1985). Crime and human nature. *New York: Simon And,*

Hindelang, M. J. (1976). *Criminal victimization in eight american cities: A descriptive analysis of common theft and assault* Ballinger Publishing Company.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and unauthorized account access. *Security Journal, 4*(1), 2-12.

IC3. (2013). *Internet crime report.* ().Internet Crime Compliant Center.

Isabella, L. A. (1990). Evolving interpretations as a change unfolds: How managers construe key organizational events. *Academy of Management Journal, 33*(1), 7-41.

Jagatic, N., Johnson, A., Jakobsson, M., & and Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100.

Jakobsson, M. (2007). The human factor in phishing. *Privacy & Security of Consumer Information, 7*, 1-19.

Jang, S. J., & Rhodes, J. R. (2012). General strain and non-strain theories: A study of crime in emerging adulthood. *Journal of Criminal Justice, 40*(3), 176-186.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566.

Kissner, J., & Pyrooz, D. C. (2009). Self-control, differential association, and gang membership: A theoretical and empirical extension of the literature. *Journal of Criminal Justice, 37*(5), 478-487.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. *Proceedings of the 5th Symposium on Usable Privacy and Security,* 3.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit,* 70-81.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT), 10*(2), 7.

Lee, A. S., & Hovorka, D. (2015). Crafting theory to satisfy the requirements of interpretation. *System Sciences (HICSS), 2015 48th Hawaii International Conference On,* 4918-4927.

Lee, S. M., Lee, S., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707-718.

Levina, N., & Vaast, E. (2008). Innovating or doing as told? status differences and overlapping boundaries in offshore collaboration. *MIS Quarterly,* , 307-332.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394.

Lilly, J., Cullen, F., & Ball, R. (1989). Criminological theory: Context and consequences.

Lowry, P. B., Zhang, J., Wang, C. L., & 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 (SSSL) model.

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and research. *Management Science, 34*(5), 583-598.

Maruna, S., & Copes, H. (2005). What have we learned from five decades of neutralization research? *Crime and Justice,* , 221-320.

Matza, D. (1961). Subterranean traditions of youth. *The Annals of the American Academy of Political and Social Science, 338*(1), 102-118.

Matza, D. (1964). *Drift* J. Wiley.

Matza, D., & Sykes, G. M. (1961). Juvenile delinquency and subterranean values. *American Sociological Review,* , 712-719.

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology,* , 417-442.

Miller, K. (2004). *Communication theories: Perspectives, processes, and contexts* McGraw-Hill Humanities/Social Sciences/Languages.

Moody, G., Galletta, D., Walker, J., & Dunn, B. (2011). Which phish get caught? an exploratory study of individual susceptibility to phishing.

Moon, B., Hwang, H., & McCluskey, J. D. (2008). Causes of school bullying: Empirical test of a general theory of crime, differential association theory, and general strain theory. *Crime & Delinquency,*

Morris, R. G., Johnson, M. C., & Higgins, G. E. (2009). The role of gender in predicting the willingness to engage in digital piracy among college students. *Criminal Justice Studies, 22*(4), 393-404.

Mustaine, E. E., & Tewksbury, R. (2007). The routine activities and criminal victimization of students: Lifestyle and related factors. *Campus Crime: Legal, Social, and Policy Perspectives,* , 147-166.

Myers, M. D. (2013). *Qualitative research in business and management* Sage.

Nagin, D. S. (1998). Criminal deterrence research at the outset of the twenty-first century. *Crime and Justice,* , 1-42.

Newman, M., & Robey, D. (1992). A social process model of user-analyst relationships. *Mis Quarterly,* , 249-266.

Ohlin, L., & Cloward, R. (1960). Delinquency and opportunity. *A Theory of Delinquent Gangs, New York,*

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in nigeria. *International Journal of Cyber Criminology, 6*(2), 1001.

Orlikowski, W. J. (1993). CASE tools as organizational change: Investigating incremental and radical changes in systems development. *MIS Quarterly,* , 309-340.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1-28.

Ormond, D., & Warkentin, M. (2015). Is this a joke? the impact of message manipulations on risk perceptions. *Journal of Computer Information Systems, 55*(2)

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *System Sciences, 2007. HICSS 2007. 40Th Annual Hawaii International Conference On,* 156b-156b.

Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology, 25*(2), 103-127.

Paternoster, R. (1987). The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues. *Justice Quarterly, 4*(2), 173-217.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review,* , 549-583.

Peel, M. (2006). *Nigeria-related financial crime and its links with britain* Chatham House London.

Prochaska, J. O., & Velicer, W. F. (1997). The transtheoretical model of health behavior change. *American Journal of Health Promotion, 12*(1), 38-48.

Puhakainen, P., & Ahonen, R. (2006). Design theory for information security awareness.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *Mis Quarterly*, , 757-778.

Rege, A. (2009). What's love got to do with it? exploring online dating scams and identity fraud. *International Journal of Cyber Criminology, 3*(2), 494.

Rowlands, B. H. (2005). Grounded in practice: Using interpretive research to build theory. *The Electronic Journal of Business Research Methodology, 3*(1), 81-92.

RSA Security LLC. (2014). 2013 A year in review. Retrieved from http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf

Salifu, A. (2008). The impact of internet crime on development. *Journal of Financial Crime, 15*(4), 432-443.

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

Schmidt, P., & Witte, A. D. (2013). *An economic analysis of crime and justice: Theory, methods, and applications* Elsevier.

Schwarzer, R. (2008a). Modeling health behavior change: How to predict and modify the adoption and maintenance of health behaviors. *Applied Psychology, 57*(1), 1-29.

Schwarzer, R. (2008b). Some burning issues in research on health behavior change. *Applied Psychology, 57*(1), 84-93.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 373-382.

Siegel, L., & Senna, J. (1985). *JUVENILE DELINQUENCY: Theory, practice, and law* (2nd ed.). St. Paul, Minnesota: West Publishing Co.

Siponen, M. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems, 7*(1), 19.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487.

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.

Sniehotta, F. F., & Aunger, R. (2010). Stage models of behaviour change'. *Health Psychology, 135*

Stack, S. (1982). Social structure and swedish crime rates A Time-Series analysis, 1950-1979. *Criminology, 20*(3-4), 499-514.

Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Strong, D. M., Johnson, S. A., Tulu, B., Trudel, J., Volkoff, O., Pelletier, L. R., . . . Garber, L. (2014). A theory of organization-EHR affordance actualization. *Journal of the Association for Information Systems, 15*(2), 53.

Sutherland Edwin, H., & Cressey Donald, R. (1947). Principles of criminology.

Sutherland, C. H. V. (1937). *Coinage and currency in roman britain* Oxford University Press, H. Milford.

Sutton, S. (2005). Stage theories of health behaviour. *Predicting Health Behaviour: Research and Practice with Social Cognition Models, 2*, 223-275.

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

The International Telecommunication Union. (2015, The world in 2015.

Tittle, C. R. (1969). Crime rates and legal sanctions. *Social Problems, 16*(4), 409-423.

Tonglet, M. (2002). Consumer misbehaviour: An exploratory study of shopliftin. *Journal of Consumer Behaviour, 1*(4), 336-354.

Tonry, M. (2008). Learning from the limitations of deterrence research. *Crime and Justice, 37*(1), 279-311.

Ultrascan AGI. (2014). *419 Advance Fee Fraud Statistics 2013*. http://www.ultrascan-agi.com/ (accessed: 30/12/2016).

Urquhart, C. (2007). The evolving nature of grounded theory method: The case of the information systems discipline. *The Sage Handbook of Grounded Theory,* , 339-359.

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

Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'theory'back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal, 20*(4), 357-381.

Van de Ven, A., & Huber, G. (1990). Longitudinal field research methods for studying processes of organizational change. *Organization Science, 1*(3), 213-219.

Vannoy, S. A., & Salam, A. (2010). Managerial interpretations of the role of information systems in competitive actions and firm performance: A grounded theory investigation. *Information Systems Research, 21*(3), 496-515.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586.

Walker, G., Adomi, E. E., & Igun, S. E. (2008). Combating cyber crime in nigeria. *The Electronic Library, 26*(5), 716-725.

Walsh, D. P. (1978). *Shoplifting: Controlling a major crime* Macmillan.

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems, 4*(2), 74-81.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *Professional Communication, IEEE Transactions On, 55*(4), 345-362.

Weinstein, N. D. (1988). The precaution adoption process. *Health Psychology, 7*(4), 355.

Weinstein, N. D., Rothman, A. J., & Sutton, S. R. (1998). Stage theories of health behavior: Conceptual and methodological issues. *Health Psychology, 17*(3), 290.

Weinstein, N. D., & Sandman, P. M. (1992a). A model of the precaution adoption process: Evidence from home radon testing. *Health Psychology, 11*(3), 170.

Weinstein, N. D., & Sandman, P. M. (1992b). A model of the precaution adoption process: Evidence from home radon testing. *Health Psychology, 11*(3), 170.

Wickersham Commission, Shaw, C. R., & McKay, H. D. (1931). *Social factors in juvenile delinquency* Government Press.

Willison, R., & Siponen, M. (2007). A critical assessment of IS security research between 1990-2004. *Proceedings of 15th European Conference on ISs, St. Gallen, Switzerland,* 1551-1559.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *Mis Quarterly, 37*(1), 1-20.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674.

Wright, R. T., & 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. 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. doi:10.1287/isre.2014.0522

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 601-610.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 Proceedings,* , 6.

Young, R., & Zhang, L. (2005). Factors affecting illegal hacking behavior. *AMCIS 2005 Proceedings*, , 457.

Zaichkowsky, J. L. (1985). Measuring the involvement construct. *Journal of Consumer Research*, , 341-352.

APPENDIX 1

TABLE 7 Summary of behavioral empirical phishing research

Study	User Base/Context	Methodology	Description	Theory Applied
Vishwanath et al. (2011)	325 undergraduate students at a US university	Phishing experiment	Proposes and tests a single comprehensive model of how individuals evaluate and process relevant phishing emails. Finding suggests that individuals focus disproportionately on urgency cues that communicate fear and threats, and in doing so, they ignore a phishing messages' source and spelling and grammar errors.	Interpersonal deception theory, theory of deception, elaboration likelihood model, and individual situational factors
Moody et al. (2011)	595 undergraduate students at a US university	Survey and "ethical phishing" experiment	Proposes and tests a model with constructs likely to predict phishing susceptibility. Finding suggests frequent Internet users are more susceptible to phishing attacks; personality traits and trust do not determine a persons' phishing susceptibility.	Personality factors (trust, curiosity, boredom proneness, entertainment drive, and risk propensity)
Sheng et al. (2010)	1,001 online survey respondents	Field study: data collected via online survey	Results suggest that women are more susceptible than men to phishing attacks; and individuals in the 18 to 25 age group are more susceptible to phishing attacks.	None
Alseadoon et al. (2012)	200 undergraduate students in a Saudi Arabian university	Phishing experiment	Findings suggest some individuals are more susceptible to phishing attacks because they are careless about trusting emails, and email experience reduces a users' susceptibility to phishing attacks.	None

Study	User Base/Context	Methodology	Description	Theory Applied
Dodge et al. (2007)	Students at a US military academy	Phishing experiment	Findings suggest phishing training had a minimal effect on respondents' phishing behavior, in the context of a relevant phishing email.	None
Wang et al. (2012)	321 undergraduate students at a US university	Field study: web-based survey	Proposes and tests a model that attempts to capture phishing design features in a relevant phishing email and individual characteristics (e.g., knowledge of phishing). Finding suggests that attention urgency cues increase phishing susceptibility, while attention to grammar errors and sender's address reduces phishing susceptibility.	Theory of deception
Wright and Marett (2010)	299 undergraduate students at a US university	Experiment	Proposes and tests a model that captures dispositional (trust, suspicion, and perceived risk) and experiential factors (computer self-efficacy, web experience, and security knowledge) likely to affect phishing susceptibility. Finding suggests that high levels of experiential factors and suspicion reduce phishing susceptibility.	Modified interpersonal deception theory
Luo et al. (2012)	105 faculty and staff members at a US university	Experiment	Proposes a theoretical framework to examine the psychological mechanism underlying the effectiveness of phishing attacks. Finding suggests that high argument quality and source credibility increase phishing susceptibility.	Heuristic-systematic model

Study	User Base/Context	Methodology	Description	Theory Applied
Downs et al. (2007)	20 non-expert computer users	Field study: data collected via email, web roleplay, and interviews	Findings suggest relevant phishing messages (e.g., recognizable brands) increase phishing victimization. Meanwhile, a sender's address and misspellings in phishing messages increase individuals' ability to detect phishing attacks.	None

TABLE 8 Background information about subjects

Subject number	Phishing emails containing threats	Gender	Age range	Education and work
1	Your account will be deactivation in 24 hours	F	30-35	Masters' degree; Social worker
2	Your account will be deactivation in 24 hours	F	25-30	Bachelor degree; Administrative assistant
3	Account deactivation notice	F	55-60	Private secretary
4	Your account has been breached	M	30-35	Masters' degree
5	Your account has been breached	F	30-35	Master's degree; Biology teacher
6	Urgent: account security update	M	30-35	Master's degree; Educational counselor
7	Urgent: account security update	M	20-25	Bachelor degree; Postgraduate student
8	Security problem with online purchase	M	30-35	Master's degree; IT consultant
9	Urgent: account security update	M	30-35	Bachelor degree; Administrative assistant
10	Your account has been breached	F	30-35	Master's degree; Counselor
11	Your account breach has been breached	M	20-25	Undergraduate student
12	Your account has been breached	M	30-35	Master's degree; teacher
13	Your account has been breached	F	40-45	Accountant
14	Your account will be deactivated in 24 hours	M	20-25	Undergraduate student
15	Your account has been breached	M	40-45	Masters' degree; IT consultant
16	Urgent: account security update	F	30-35	Masters' degree; Finance
17	Urgent: account security update	F	25-30	Bachelor; Engineer

TABLE 9 Example of coding

Subjects	Exemplar texts	Open codes	Selective codes	Theoretical codes
Subject 16	I first started using the email account in 2009. I opened the email account when I started using the Internet. Back then, having an email account was trendy; everyone was using email. So, I also decided to open an email account. However, I was not used to it so I think I am now using my third email account. The earlier ones have been closed. I decided to have an email account in order to easily and quickly connect and communicate with people and with my friends and family in distant places	Using email accounts Trendy Using email for connecting with family and friends	Uses of personal email accounts	The nature of email use
Subject 7	I am nothing without my email account. My Yahoo account is private; I use it for my personal affairs. Acting to protect my account helps to secure my financial transactions. I do several financial transactions through my email account	Importance of email account. Email account is private. Personal and financial transactions	Personal nature of email account and use	
Subject 13	My decision was influenced by my knowledge at the time about security and privacy on the Internet. My friend told us that his account was hacked, and he started receiving sexually explicit messages and pictures. That is an embarrassing thing to happen to someone. So, of course, I was concerned that something embarrassing might happen to me. Always best to prevent such an occurrence if you can	Online security and privacy knowledge Concern for information security and privacy Fear of embarrassment Acting to avoid information security violation	Information security and privacy concerns	Information security and privacy concerns

Subjects	Exemplar texts	Open codes	Selective codes	Theoretical codes
Subject 3	When I got this email that said my account will be deactivated, and that I must act by a deadline, I first ignored it. I knew there were dangers in having an email account and using the Internet. However, I didn't know that I was personally vulnerable to those risks. Yet, I also didn't want to lose my account, so as the deadline approached and the message was still sent to me again as a reminder, I felt pressured and fearful that I might lose my account. I filled in the form and gave my username, password, secret question. I share little gossips here and there; work gossip with colleagues about our bosses. Something bad happens to my account, someone accesses it and our bosses discover it, I will be so ashamed. And maybe I can lose my job. Or what will my other colleagues be thinking of me? That it's my fault? No, I had to do something	Account deactivation notice Avoiding loss of email account Protecting online gossip and self-image	Protecting personal email accounts Concerns for personal transactions	Protecting personal transactions
Subject 5	The phishing email stated that my account has been breached. In my email account, I have different kinds of relationships with my friends. We discuss different kinds of private chats. It can be embarrassing if the things my friends share with me and I with them were exposed to everyone. What do I tell them? I also have my own secrets in those conversations. Given that it says hackers breached my email account, I worried they can further blackmail or threaten me. I feared that they will threaten to expose everything about me and bring shame on me and my friends. With these thoughts going through my head, I knew I had to act	Account has been breached Keeping chats private Secrets Privacy protection against blackmail Protection motivation	Protection motivation behavior	

APPENDIX 2

TABLE 10 Summary of previous scamming research in information systems

Study	Objectives	Findings
(Herley, 2012)	Examined Internet scam websites using a mathematical model to understand why Internet scammers broadcast that they are from Nigeria.	Found that Internet scammers use this strategy to maximize their profits, ensure that non-gullible Internet users who are difficult to manipulate do not respond, and to reduce the cost of follow-up emails.
(Abia et al., 2010)	Examined why young people in Cameroon become Internet scammers. They administered questionnaires to students aged 12 to 25 years, a majority of whom were friends of Internet scammers.	They reported the need for money, peer influence, and prestige and unemployment as the most common reasons for becoming an Internet scammer.
(Burrell, 2008)	Examined Internet scammers' complicity in using IT to perform Internet scams. Study is based on interviews with Internet scammers, Internet café owners, Internet users, and relatives of Internet scammers.	Found that scammers misrepresent themselves to get attention from disinterested Western audiences, and they unite their own self-interests with the interests of their audience.
(Boateng et al., 2011)	Examined the different forms of cybercrimes in Ghana, and how Ghanaian authorities are dealing with its prevalence. Study participants included victims of Internet scams, cybercafé owners, and bank officials.	They found that Internet scamming is prevalent in Ghana, that Internet scammers are young and have university level educations, and that victims do not report being victimized because of a lack of confidence in the legal process and a fear of embarrassment.
(Chang, 2008)	Examined how Internet scams operate by studying six Internet scam emails the authors received in their regular email accounts. The goal was to identify the methods scammers use to deceive victims.	Their interpretation of the emails suggested that Internet scammers exploit victims' bounded rationality using authority, expert power, and believability in the advance fee fraud emails studied.
Karger (2004)	Examined the fringe economy (e.g., predatory lenders in the USA) and the strategies used to scam people in low-income communities.	Payday lenders, tax refund outlets, etc., use their legal status to deplete almost 10% of the value of a low-income family's tax refund through tax preparation fees and refund loans.

Study	Objectives	Findings
(Atta-Asamoah, 2009)	A research commentary on one approach to the Nigerian 419 scam.	The author claims that Internet users expose themselves to scams and recommends education, web-based education, legislation, and international cooperation.
(Ojedokun & Eraye, 2012)	Collected data from a general university student population to understand their views on university students practicing scams.	Found that others perceive scammers as extravagant and that scamming has a negative effect on academic performance.
(Walker et al., 2008)	Reviewed the state of AFF scams and efforts to combat AFF scams in Nigeria based on freely available documents on such scams.	Concluded that, while the Internet provides economic benefit, it is aslo a major cause of financial harm. Found that the Nigerian government has created structures such as the central cybercrime agency for combating AFF scams.

TABLE 11 Exemplar interview transcripts

Stage 1: Origin of the Problems			
	Loss of Business Income	Open Codes	Selective Codes
Subject 1	I was a hawker, selling insects to tourists visiting Cameroon. After a successful sale, I encouraged my customers to recommend me to their own friends who might be interested when they return to their home countries. Soon, all these new overseas customers were simply saying the same thing: they only wanted to buy at unreasonably low selling prices. In addition, the selling price they demand does not include any shipping costs. I started feeling that these customers just don't care. The customers are racist; they think that because I am African, any price is good enough. There were also many people who had joined the business to supply insects and other exotic amphibians. Thus, my customers had many suppliers to choose from; I think this encouraged the customers to make demands. If I ask them to pay a better price, the customers simply switched to another supplier, or say my items will rot in the forest.	Unreasonably low selling prices, greedy customers, competitive market with many suppliers, pre-scamming activities: hawker.	Loss of business income.
Subject 2	I graduate from university. I can't find a job and decide to open a garage in order to sell secondhand car parts. It is a dirty business. I was always covered in oil and I always smelt engine oil. The tax officials are there for themselves, they don't care about anyone. I can't find a job, I tried to be responsible and do something to help myself, my family, and my countrymen. Yet, the government doesn't care. If you don't have a god-father, you end up with nothing. The system is about cheating to get your way. I paid taxes but I was frustrated by the fact that I had to pay bribe for my taxes to be signed. I went to the tax office and I was told that I must give a bribe before I can be classified into a lower tax category. I was mad. I went to see the head of that tax division and he only said I just have to comply. Even online, one of my overseas suppliers dubbed me. He took my money and did not supply me with the goods. That was it. I had had enough. That was the game changer as I was really angry and frustrated. I was going to get my revenge by cheating for a living too.	Corrupt tax officials, government ineptitude, dishonest supplier, anger, frustration, revenge, secondhand car parts shop/garage.	Loss of business income, negative emotions; pre-scamming activities.

Subject 3	I tried running a video club business, and a long time I was successful. I opened the video club on 21st October 1994 and closed on 19th September, 2005. Around 2002 cable television and cheap DVDs started entering the market. The DVDs came from china so they were very cheap; people could buy them and then rent the latest movies. My business just couldn't compete. Cable TV channels also showed some very new movies. Cable TV was also playing the movies we were playing in video clubs. After I closed my business, a friend introduced me to the sale of reptiles, amphibians, and snails. I have been doing this business for 6 years. I know about snails. I have customers in Canada. Then, I started working at a cybercafé. I heard scamming from the cybercafé. I went to google and searched. I learned the scamming part online on my own. The economy is tough and the income from scamming helps. I tried running a video club business, but taxes made me to run so I started the scamming. So, my business crumbled. I started collecting people's money when I didn't supply a product. I felt bad, I took money in the hope of supplying the merchandise later. Sometimes, my customers want a product that I don't have. They know I have a good reference from another customer. When I receive the money upfront, I have scammed him. I will lie that I have the product.	Change in market environment, poverty, video club, work at cybercafé, supply of merchandise, feeling remorseful.	Loss of business income, pre-scamming activities, remorse.
	Friends Become Internet Scammers		
Subject 10	I was taught scamming at a cybercafé. After I made some money I bought my own laptop and personal Internet access. I became a scammer because of my close friends. At times, when we went to read, they would also want us to go for drinks. I always lacked money, and my friend would always buy me and my other friends who were not yet scammers drinks. He did that on many occasions but at one point, he said that I can't just be consuming and that if I want to go out and drink, he will teach me scamming. I was interested, and I asked him to show me how I can make my own money. I met him at his home because he has a laptop and Internet connection at home. He introduced me to the websites and Facebook. I love the lifestyle. This lifestyle started with my friends. Before scamming, my friends did not have money. But they had another friend who was already a scammer, and he introduced them into scamming.	socializing with close friends, lack of money, interest, financially independent, love of the lifestyle.	Friends became Internet scammers, money, scammer lifestyle.
Subject 7	I have been doing scamming since 2011. I am a university graduate. I have a law degree. I joined scamming because I lived in an environment where most of my friends were scammers. I was never interested. So, I completed high school and enrolled at the	Student, friends became scammers, cost of	Cost of scammer lifestyle, money.

	university in 2010. The general idea is that is hardship that drives everyone to scamming. But first, as I went out with my friends, I needed to also meet up with the expenses. My mum who used to assist me was sick but older siblings were not financially assisting me. My family noticed that I was buying expensive phones and spending money and demanded to know. I openly declared to them that I was a scammer. They were not willing to assist me when I needed their help most. Before scamming, I regularly frequented the Internet to communicate and play games. I was living a normal life, and I was happy until I discovered that money is more important to girls; I also discovered that even people who are uneducated can have better lives from scamming than from studying. The person who has more money has more respect than the educated but financially broke person.	lifestyle, lack of money, money brings respect.	
Subject 5	I first accessed the computer in 2003. After I completed university, I couldn't find a job so I did a professional computer course. I learned computer maintenance and networking. Then, I met some friends who were scammers, and they proposed it to me. Started scamming when unemployed.	Unemployed university graduate.	Money
Subject 9	I have been doing scamming for 4 years. I started after my high school diploma. When I enrolled at the university, my friends were already living big and partying. I joined them, but I could not meet up with the expenses. I don't come from a wealthy family so to meet up with my expenses, I chose to become a scammer. 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 wasn't even familiar with the computer. My friend taught me about computers, how to place your ads, if you have a contact, how you would reply, and if the target contacts you, he taught me how to react, what to say. I learned how to scam in a cybercafé. If not for my friends, I might not be a scammer. They influenced me significantly.	Student, friends became scammers, good lifestyle, friends, learned from friends.	
Stage 2: Solution			
	Context of the Solution		
Subject 11	I have been doing scamming for five years. Whether it becomes my permanent career depends on how things turn out. I joined because I finished school, and I couldn't find a job. In 2010, I was learning driving at OIC (a local vocational school). I finished and after six months I still didn't have a professional job. I traveled for some job interviews to another province for a month. Upon my return, all my friends were at cybercafés	Unemployed graduate, spending more time online with scammer friends,	Guilt

	doing scamming. They had become scammers while I was away. I would stay at home doing nothing while they worked at a cybercafé. Then, when they came, they mostly had money, and I was the only person without money. I was reluctant to join because I knew it was wrong. But after a while, the feeling of loneliness, they had the latest gadgets, I had nothing. So, I decided to learn and become a scammer. I was only interested in scamming after my friends joined. We grew up together, and when I entered their homes, they had all these nice gadgets. I overcame the guilt to join scamming because of loneliness and poverty.	scamming is wrong.	
	Solution to Their Problems		
Subject 9	Facebook has made scamming easy because when we posted our ads on classified ads, you could stay for days, with just one or two contacts. But with Facebook, as you post your ad on a certain group that contains 4,000 people, you realize at the end of the day, you have about 50 contacts, within those contacts, you can have serious conversations with 4 or 5 people. Plus, we are doing live chatting and that makes the conversation easier and faster. But now Facebook has updated its policy because of scam reports. If they suspect you are just joining groups, your account is shut down and that is really boring.	Using Facebook to post scams versus using classified ads, benefits of Facebook (live chatting, faster communication), deterrence by Facebook to reduce scammers' activities.	Misrepresentations through a computer-mediated environment.
Subject 6	I deal in puppy because it does fast money, I have never seen these puppies with my own eyes. I make an advert that says, I am offering the pet for adoption. I don't say I want to sell. We know the puppies they like and we search their pictures on the Internet and say we have them for adoption. We have a first mail, second mail, and third mail. We have another address say airport. We post our ads on Facebook. We go to Facebook, and type sales in Texas, options appear, choose sales in Texas. Once I am approved for a group, I start posting your adverts and those interested will contact me. I also sometimes use IPS, which are websites you can buy. Now, however, scammers prefer Facebook.	Fast money, customers' preferences, planning of scams, prewritten letters.	Preferences
Subject 10	Operating as a scammer requires working with a lot of ideas, and you can't have those ideas alone. So, I learn from others, and they learn from me. We share ideas. You can't	Learning how to commit scams	Learning to commit scams

	know everything, and there are different stages of scamming. But in my own stage, most of the things I do, I do by myself. I only work on Facebook. I am at the lower stage, and this is different from those who do company scamming, e.g., companies that need palm oils in thousands of liters, and you need to prove that you have that quantity of oil through pictures and a lot more documentations. There are much older scammers who have done this higher-level scamming for long, and I will need them to help even teach me to get to their level. They will mentor me for free or give me the types of documents I need to work with for free. I will have to make an agreement with them that if the deal is successful, they will receive about 30 percent. These guys are at the highest stage of scamming. He may assist with any problems I have.	from other scammers, learning from more experienced scammers, justification: lower-level scams versus company scams as justification.	online, justifying committing scams.
Subject 5	He contacted my ad and asked about the puppy. I said I was giving the puppy adoption, he was interested, and I said I will need money to pay for the flight and logistics, and he can send the money, and I will send the puppy. I did fake documentation, e.g., fake tickets and he sends money thinking it was to the flight agency.	Using adoption as a form of persuasion; reasons for advance payment.	
Subject 5	After I did pet scams for a while, I moved on to doing fertilizers as I discovered that advertising and pretending to sell bulk products makes more sense. I got a customer who wanted to buy two containers of fertilizers and the amount was about CFA 6 million FRS. That was my best experience to date. To me, the victims are greedy, greedier than us. They know the market price of these products, and if you give them the actual price they don't contact you but if the price is low, they don't contact you.	Transferring scamming skills, doing other types of scams, justification: blaming the victims, victims are greedier; they prefer lower selling price.	
Stage 3: Persisting in Scamming			
	Justifying the Solution		
Subject 10	I know older scammers who have made CFA 100 million FRS, and I after a few days or weeks they are begging for CFA 100 FRS. The extravagant lifestyle is part of scamming. If I scam, my first thought is to spend on clothing, clubbing, girls. After two days, the money is finished. I wouldn't even think of investing. The question of what we do with	Extravagant lifestyle, cost of lifestyle, scamming	Justifying committing scams.

	the scamming money is really haunting me. I think that when I compare myself to my non-scammer friends who are doing genuine things, they are better than me. Even though I am now popular, and sometimes wear nice clothing that most people would appreciate, those my non-scammer friends are better than me. Because now that scamming someone is a bit hard, I meet with them and tell them, 'men, it's not working.' They don't live extravagant lives, or go around getting drunk. They have already graduated from university. I still have one more year because of scamming.	money, popularity.	
Subject 6	When someone shows interest, I send the information about the puppy: where it lives, how it interacts, what it eats, and vaccines I have administered. The information I provide helps them think I know and am serious about the puppy. When the interested 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 make money through the delivery, so the customer will request that I should deliver the merchandise. When the customer replies to the second email, I send him the third mail which includes my legal address, real name, country (Cameroon), country code, and there you have a 75% guarantee that he will make the payment. It is important that he adds Cameroon. When he goes to the bank, to collect the money, they sometimes know that it is a scam, and some bank tellers can ask for a bribe before effectuating the payments. When I receive the first payment, I ask the victim to pay insurance to guarantee a safe arrival of the puppy. Then, he will contact me on Facebook to complain that I didn't tell him about insurance and I have to convince him. Victims are becoming more aware and they identify scam attempts and report us on Facebook. Facebook blocks you after you post an advert on ten groups. So, we only post on say two groups each. Since there are thousands of individuals in each group, we are hoping that someone will likely initiate a contact. The government policy is very ineffective. When the police they are asking for their own share of the scamming proceeds. The corrupt police catch us through the scamming money. Most often, when the police come after immediately after I have collected your scamming money, it only means another scammer has informed them. Our scammer friends who are jealous collude with the police. So, it's best to keep quiet about your success until you have the money with you.	Planning of scams: falsifying location, misrepresenting international travel organizations, justifying payment to Cameroon, persuading victims to ignore advise from bank tellers, persuading victims to make multiple payments, victim awareness of scams, deterrence intervention by Facebook, ineffectiveness of government policy, corrupt	Deterrence measures, deterrence effectiveness, local context.

		law police officers, collusion between scammers and law enforcement.	
Subject 7	At times, we say we don't care. We say, if I have to feel sorry, it should only be after I have the money in my pockets. But when I am alone, I have some time to reflect, to meditate over my life, and when you are alone to reflect, many things come inside my mind, you don't only think about yourself and your family, you think about those you are hurting. At times, it really hurts, I know that one day it's going to fall back on me as karma.	Timing of remorse, karma.	Karma, nature of remorse.
Subject 12	I have made CFA 1.5 million FRS and I am still in scamming. I don't know why. Before I have the money, I have some very concrete plans, like opening a business. However, when I have that money, I don't know if it's the law of karma but I spend the money and nothing good comes out of it. Then, the extravagant lifestyle seems to also make more sense. We are also used to a particular lifestyle and to abandon it might not be easy. I can blame myself because no amount of hardships. I am praying for deliverance from God. I have a degree and have no job.	Karma, extravagant lifestyle, plans to quit, challenge of quitting.	Justifying committing scams.
Subject 7	I denied scamming money once. Well, it was not a lot of money. But this lady, after she discovered that she had sent me every money she had for scam, she snapped a picture of her children who desperately wanted the pets she had paid for. She had spent all her money, and they still didn't get the pet. The children in the picture were crying and she said they are crying because they want the pet. The money was GBP 75 pounds. I abandoned the money at Western Union. I just felt some remorse. When I told my friends, they were really disappointed with me. They said I was putting the victim first. You see, the game – scamming – must always come before the victim. Because first, if you are doing scamming to get money, which is the game, everything must come after the money is in my pocket, that is the psychology we have.	Effect of victims' discovery of a scam on scammers, scamming trumps feelings of remorse/guilty conscience.	
Subject 11	I feel guilty but I find ways to console my myself. I feel guilt for some specific victims. Some are wealthy, but others are not, and they really cry about the money. But I also	Feelings for victims.	Remorse

	need it because of my own condition. Because I am hurting someone. Especially those I discover lack and complain that they need the money for their children.		
Subject 7	I don't see it as a big deal to break the law in Cameroon. So, scamming being illegal here is not a problem. Everyone is somehow corrupt. If I am caught, the police will ask for their share; that is, their own percentage. So, I don't think about getting caught because I can find a way out if I am caught. That said, the greatest threat to scammers is our fellow scammers. Scamming is a game, and sometimes we have conflicts among scammers.	Justifying scamming through government corruption, scammers as a point of deterrence.	
Subject 9	I trying to complete my university degree. I want to quit scamming and the way out is through completing my studies. It is not easy to manage both because both need a lot of time; so, I am doing scamming part time. My studies can actually make me a more proficient scammer, but my aim is not to continue in scamming, but to do something more honorable. Nowadays, most of my friends' names are on scam alert lists in the Internet. So, we use a pickup to collect the money from the bank. We can fake names for email addresses, but when it comes to names for payment, you have to use the real name because you are doing banking; you have to identify yourself.	Justifying through plans to quit, fear of being blacklisted, use of pickups.	Pickups, deterrence
Subject 6	I was aware of the risks. 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.	Avoiding detection by operating from private locations, technological infrastructure as hampering deterrence measures.	
Subject 7	I learned from my friend. He taught me scamming from his laptop at home. My friend who taught me scamming only taught me about dating scams. Nowadays, I have laptop so I do my scamming at home. Among my age group, we mostly work at home because the cybercafés are congested with those younger ones 15 years.	Operating from anywhere, avoiding cybercafés.	

TABLE 12 Comparing the new and old generations subjects

Themes	New generation	Old generation
Differences		
Pre-scamming activities	Jobs: none; Work skills and experiences: none Other activities: attending school and socializing with friends	Jobs: Employee at a cybercafé, shop managers, hawker,
Motivations	Friends, friends' newfound scamming lifestyle, money	Stressors from business failures (anger, frustration, revenge), money, competition, poverty
Nature of interactions with mentors/teachers	Close, intimate, and social interactions with friends	Distant and opportunistic
Learning behaviors	Intimate social learning, direct observation and learning by doing	Direct observation, self-learning (trial and error), learning by doing
Practicing scamming	Meeting Short-term goals, delayed timing of remorse/guilt, corruption, poverty, karma, lifestyle, meeting long-term goals, using of pickups, ineffective deterrent interventions, perceive some victims as wealthy	Blaming the victims, corruption, long-term career, anger
Similarities		
Persuasive strategies	Demonstrate desperation, Careful design and posting of scamming ads, sound and appear authentic, demonstrate expert knowledge, interaction skills, use of prewritten letters, document fraud, social persuasive skills	
Information technology	Using false location, facilitating/enabling the persuasive strategies, using multiple email addresses/Facebook accounts,	

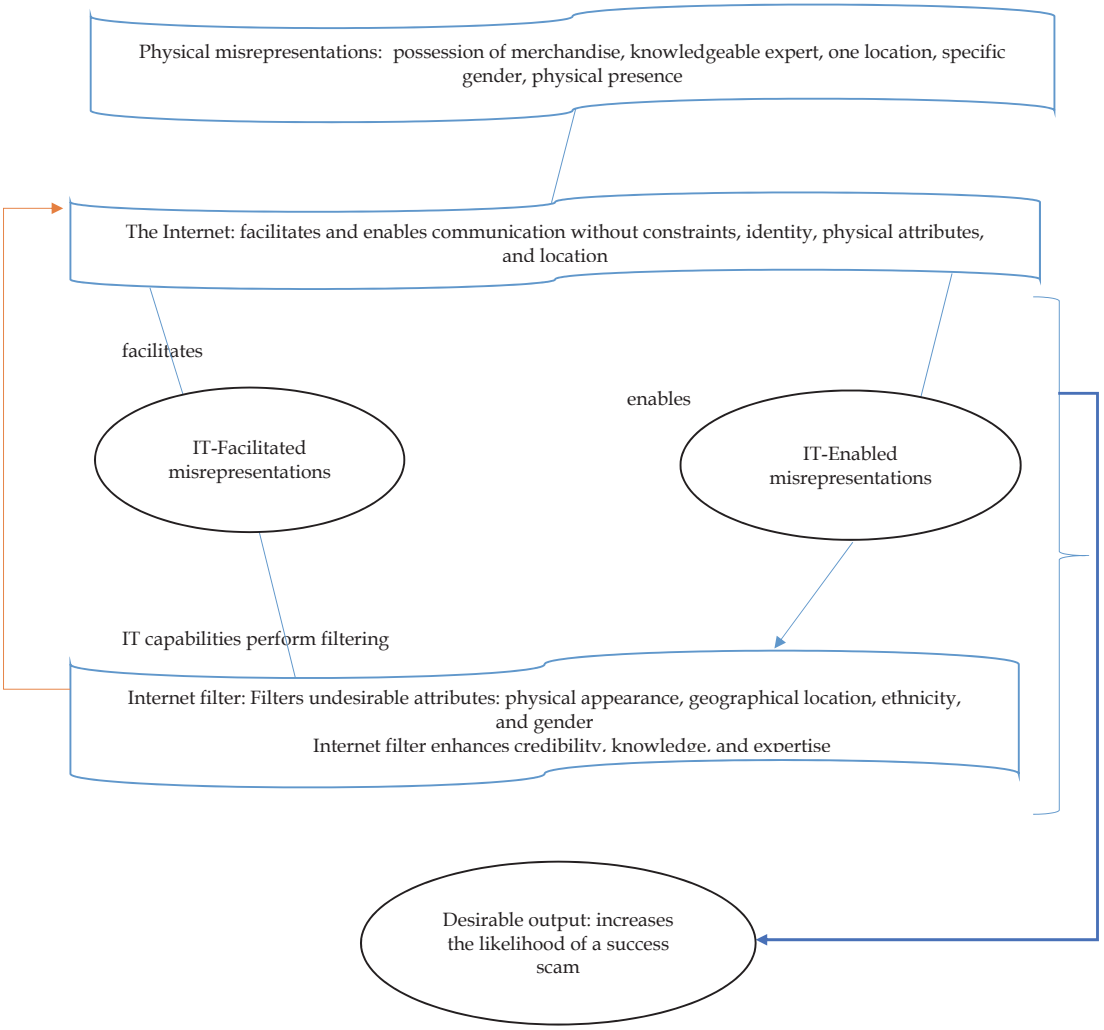

FIGURE 2 Misrepresentations through the Internet