Understanding Internet Fraud: Denial of Risk Theory Perspective

Martin Offei[1(✉)], Francis Kofi Andoh-Baidoo[2], Emmanuel Ayaburi[2], and David Asamoah[3]

[1] Koforidua Technical University, P.O. Box KF 981, Koforidua, Ghana
martin.offei@ktu.edu.gh
[2] University of Texas Rio Grande Valley,
1201 W University Drive, Edinburg, TX 78539, USA
[3] Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

Abstract. Internet fraud has become a global problem attracting the attention of researchers, practitioners and policy makers. Existing empirical theoretical studies on internet crimes have mostly used neutralization and deterrence theories. Despite the insights from these theories, we are still observing an increase in the number of internet crimes. We argue that Denial of Risk theory may provide new insights on internet crimes such as internet fraud. We examined how each of the three dimensions of Denial of Risk theory (scapegoating, self-confidence and comparing of risk) serve as antecedent of the intention to commit internet fraud. Using responses from 350 individuals from internet fraud hotspots, we showed that scapegoating, self-confidence and comparing of risk are positively related to intention to commit internet fraud. The study offers theoretical and practical contributions to research in the spectrum of internet fraud and the theoretical application of denial of risk in cybercrime research.

Keywords: Internet fraud · Denial of risk theory · Scapegoating · Self-confidence · Comparing of risk

1 Introduction

Cybercrime has become a global issue as it affects individuals, businesses and governments everywhere including developing economies (Chatterjee et al. 2018; Li and Cheng 2013; Shareef et al. 2018). Examples of cybercrimes include identity theft, piracy, hacking and financial fraud committed over the internet. We focus on internet fraud in this research because such crimes affect a wide audience and perpetrators are usually anonymous. Internet fraud is broadly described as crime perpetuated on the internet components such as web sites, chat rooms, and e-mail, to offer non-existent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims' funds, access devices, or other items of value to the control of the scheme's perpetrators (Kubic 2001). Internet fraud appears in diverse forms such as "skimming, Card-Not-Present (CNP), stolen credentials buyers, professional hackers/crackers, identity theft" and among others (Boyle and Walker 2016, Jegede et al. 2016a, b).

Published by Springer Nature Switzerland AG 2019
Y. Dwivedi et al. (Eds.): TDIT 2019, IFIP AICT 558, pp. 415–424, 2019.
https://doi.org/10.1007/978-3-030-20671-0_28

Most prior research have used theories such as neutralization, deterrence and motivation to extend our understanding of internet crime phenomenon (Lazarus 2018). In general, these theories assume the individual appreciate the enormity of their crime or severity of the punishment. We argue that the increasing number of internet crimes despite the recommendations from prior research is because those individuals involve do not envision any risk in their quest to defraud unsuspecting victims. This is because most individuals involved in internet crime believe they cannot be located due to the anonymity and vast size of the internet. Employing a risk perspective, this study seeks to understand the internet fraud phenomenon. Specifically, we seek to answer the following research question: What risk perception factors influence individuals who intend to commit internet fraud?

This research seeks to make theoretical and practical contributions to research in the spectrum of internet fraud by using denial of risk theory as its basis. Denial of risk theory refers to the cognitive way individuals deal with risky behaviors by rejecting the presence or effect of risk (Peretti-Watel 2003). We developed a research model to understand how risk perception influence individuals' intention to commit internet fraud using components of denial of risk theory. We collected data from 350 individuals located in internet crime hotspots on key constructs, denial of risk and intention to commit internet fraud in our model. The results of the analysis of response data offer both theoretical and practical implications. For theory, we have shown the efficacy of Denial of Risk theory in understanding burgeoning Internet fraud discourse. For practice, our study provides insights for law enforcement agencies to understand the factors that act as drivers of internet fraud.

2 Theoretical Background – Denial of Risk Theory

Denial of risk refers to cognitive ways to develop adaption to risky behaviors by rejecting the possibility of suffering any loss (Peretti-Watel 2003). The theory posits that an individual may deflect the level of risk by comparing the crime to an acceptable action they consider a crime. The theory of denial of risk has three main constructs: scapegoating, self-confidence and comparing of risk. Scapegoating is when an individual stereotype actions of others they consider harmful (them) relative to their behavior. For example, young drivers label (scapegoat) older drivers as overly cautious as a justification for their over speeding habit. Self-confidence is when an individual reject risk by distinguishing themselves from anonymous group. For instance, some drivers who overspeed justify their action by suggesting that they possess better driving abilities than an average driver on the road. Comparison-between-risk arises when an individual compares their actions with that of a group whose action are already accepted. For example, individuals who text-while-driving may deflect risk by suggesting that driving-while-using-wireless communication is equally risky as individuals in both situations are affected by the information been communicated. Denial of risk theory has been used in the criminology literature to understand why individuals commit crime such as the use of cannabis (Apostolidis et al. 2006). We argue that each of these dimensions of denial of risk theory may influence an individual's intention to commit internet fraud because of the anonymity provided by the internet.

Internet fraud involves the use of internet and related activities that violate the ethical conducts of the internet (Kubic 2001). Internet fraud is of concern globally for governments and law enforcement agencies (Grabosky 2015). Internet fraud is perpetuated by individuals or groups of individuals with different backgrounds such as needs, education and cultural idiosyncrasies (Morris and Higgins 2009). The techniques used by perpetrators of internet fraud make them believe the consequences of their actions are less harmful and sometimes beneficial to the victims (Brooks 2016). We employ the three dimensions of denial of risk to develop a conceptual model that explains intention to commit internet fraud.

3 Conceptual Model Development

Scapegoating

The scapegoat construct of the denial of risk theory deals with the propensity to label an identifiable group as taking actions that are deemed riskier (Lazarus 2018). Employing scapegoating technique results in feelings of prejudice or stigmatization toward the person or group that one has accused of committing crimes that are relatively harmful. It provides the basis for the perpetrator of the crime to deflect any risk arising from their actions, thus resulting in positive self-image (Harris and Dumas 2009; Lazarus 2018). For instance, individuals who are engaged in internet fraud feel they are not causing harm to their victims' relative to harm caused by hackers who alter or prevent victims from continuing their normal lives. For instance, some cybercriminals in developing nations have believe that criminals in western countries cause more harm to their victims than they do (Hutchings 2013). Such rationalization of the risk of committing internet fraud transforms risk into blame (Sugiura 2018). The criminals use scapegoating to absolve themselves from their criminal behavior. Thus, we posit that:

> ***H1:*** *Scapegoating as a technique of denial of risk positively affects the intention to commit internet fraud*

Self-confidence

Self-confidence is the cognizance that makes one believe in their abilities to perform certain tasks without much difficulty. The self-belief in a confident person is very high and rises with more complex task such as creating situations that makes it easy to defraud another person. Self-confidence helps individuals to participate in the crimes they commit (Sigala 2017, Jegede et al. 2016a, b). Although individuals know that they are committing a crime that is punishable by law, they deny this risk by showing confidence they will not be punished. Sometimes perpetrators of internet crimes draw solidarity among themselves to increase their confidence level (Jegede et al. 2016a, b; Koay 2018). Therefore, it is posited that:

> ***H2:*** *Self-confidence as a technique of denial of risk positively affect the intention to commit internet fraud*

Comparison Between Risks. Comparing of risk looks at the lesser evil perceived by the perpetuator of internet fraud. Individuals who commit internet fraud compare their activities to other crimes such as hackers or identity theft and perceive that the activities they are involved in are better evil (Choo 2011). By comparing the risk of their crimes, criminals perceive some crimes as much riskier than others.

It is reported that some individuals who are engaged in internet fraud compare the crime to other crimes such as stealing and cheating and perceive that such crimes are not less harmful when compared to what they do (Mekonnen et al. 2015). Individuals who commit internet fraud are shielded in the comfort of anonymity. Such individuals proclaim and perceive they are far away from the victims they defraud and believe that they cannot be caught or punished (McMullan and Rege 2010). Therefore, it is posited that (Fig. 1):

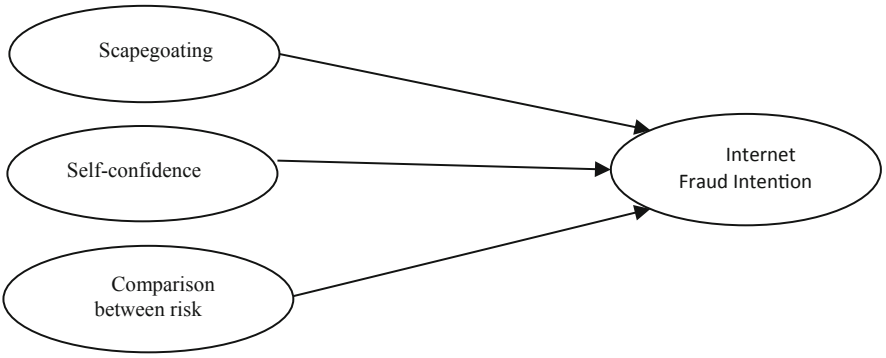

Fig. 1. Research model

H3: *Comparing of risk as a technique of denial of risk positively affects the intention to commit internet fraud*

4 Methodology

Measures and Sample

This study was conducted using a survey research design (Choudrie and Dwivedi 2005). The target population for this study are individuals located in alleged hotspots (internet cafes) where internet fraud originates (Odou and Bonnin 2014). Unique high unemployment in some of these regions encourages internet fraud (Smith et al. 2001; Boateng et al. 2011). Due to the heterogeneous and illegality of the phenomenon understudy, the total population of the study is not known. Our sample included 350 respondents. The sampling techniques used in this study are cluster sampling, convenient sampling, and snowball sampling approach. Cluster sampling are the regional distribution of internet fraudsters within Ghana. The clusters represented internet fraud hot spots within the selected regions (Greater Accra, Eastern, Volta, Ashanti, Central

and Western), convenient sampling was used to select a section from each cluster in the internet fraudsters' cafes. Furthermore, snowball sampling technique was used to identify other individuals suspected to be involved with internet fraud and online relationship scams.

We adopted 12 items from Peretti-Watel (2003) to measure scapegoating, self-confidence and comparing of risk. These items were used in prior study to juvenile intent to commit an illegal act -weed smokers- in France.

Our dependent variable, Internet fraud intention was operationalized as a second order construct consisting of two first order constructs (deception and fraud). The 8 items used to measure our dependent variable were adopted from (Park and Sung 2015; Siponen and Vance 2010). Details of the measures used in the study along with their loadings are presented in the appendix.

5 Results and Analysis

The Structural Equation Modeling (SEM) was used to investigate the causal paths hypothesized in this study. A two-step approach was used to analyze the data. In the first step, the covariance-based technique was used to assess the appropriateness of the measurement model. The covariance based technique was used as it minimizes the differences between the covariance of the collected sample and that of the ones predicted by the model and reproduces the covariance matrix of the observable variable. For testing the structural model, variance based partial least square (PLS) SEM was used as it maximizes the variance of the dependent variable which is explained by the independent variables.

We used the Cronbach Alpha, Composite Reliability and Average Variance Extracted (AVE) to test for reliability and validity of the constructs. Discriminant validity tests were performed to test for accuracy of the measurement items by using Fornell-Lecker Criterion and Heterotrait-Monotrait (HTMT). A HTMT is a more resilient test for discriminant validity than cross loadings. As shown in Table 1, constructs reliability are confirmed as composite reliability (CR) values for all factors were above the recommended 0.7 value threshold, indicating item consistency. The variance explained (AVE) is above the satisfactory threshold of 0.5, confirming convergent validity.

Table 1. Construct validity

	CR	AVE	CA	DorCr	DorSc	DorSg	IcifDp	IcifId
DorCr	0.833	0.625	0.842	**0.79**				
DorSc	0.878	0.705	0.724	0.214	**0.84**			
DorSg	0.874	0.699	0.790	0.222	0.971	**0.836**		
IcifDp	0.882	0.652	0.775	0.179	0.417	0.428	**0.807**	
IcifId	0.866	0.684	0.689	0.265	0.116	0.143	0.225	**0.827**

DorCr - Denial of risk-Comparing of risk, DorSc - Denial of risk-Self-confidence, DorSg - Denial of risk - Scapegoating, IcifDp - Intention to commit internet fraud-Deception, IcifId - Intention to commit internet fraud - Defraud

We conducted model robustness checks for multicollinearity. VIF values for scapegoating (2.04), self-confidence (1.937), and comparing of risk (1.5) are much less than the threshold of (VIF < 10), indicating absence of multicollinearity problem. In assessing the explanatory power, our model accounted for 58% of variance ($R^2 = 0.58$) in explaining intention to commit internet fraud.

The Adjusted R^2 (0.56) further strengthens the explanatory power as it takes into account our sample size and number of variables in our model. Summary of the hypotheses testing are shown in Table 2 and Fig. 2.

Table 2. Summary of results

	Hypothesis	Support?
H1	*Scapegoating positively affect the intention to commit internet fraud*	Supported
H2	*Self-confidence positively affect the intention to commit internet fraud*	Supported
H3	*Comparing of risk positively affect the intention to commit internet fraud*	Supported

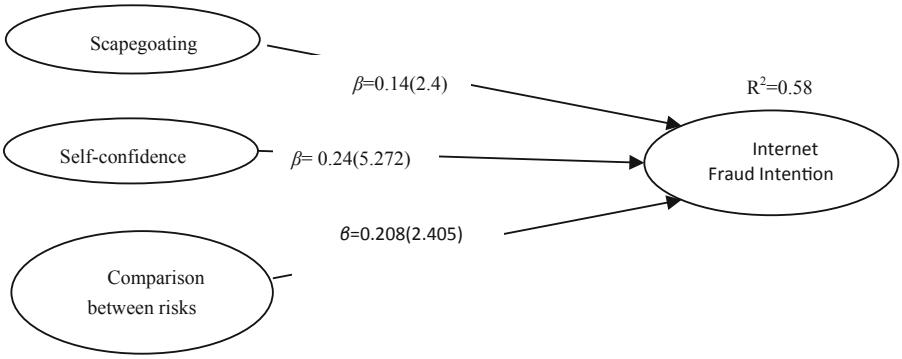

Fig. 2. Model results

As hypothesized, internet fraudsters use scapegoating to commit internet fraud ($p < 0.05$; $t = 2.44$), and hypothesis 2 supports a positive relationship between self-confidence and intention to commit internet fraud ($p < 0.05$; $t = 5.272$). Hypothesis 3 is also supported ($p < 0.05$; $t = 2.405$); comparing of risk positively influence the intention to commit internet fraud.

Discussion and Future Research Direction

Denial of risk theory refers to a mental way to deal with risk associated with deviant behaviors. Individuals who employ denial of risk attempt to reject the risk from the actions by comparing their actions to others who they deem more harmful. We used this theory as the basis to understand the intention of individuals to commit inter fraud that is regarded a harmful or unethical use of computers. We argue that internet fraudsters

justify their deviant behavior by using these techniques to justify their behavior. Internet fraudsters persuade themselves they are anonymous and law enforcement are incapable of apprehending them. In societies where risk is downplayed, denial of risk theory offers an understanding of how these internet fraudsters view their risky actions by scapegoating, self-confidence and comparing of risk. This complements research on cybercrimes that have used neutralization and deterrence theory by suggesting the increase in internet fraud, a form of cybercrime, should be looked from denial of risk perspective.

The findings of the research are consistent with prior studies on denial of risk theory such as Peretti-Watel (2003) study on use of cannabis among young smokers. The publicity of arrest of individuals involve in internet fraud may have no effect on the number of internet crimes committed. One explanation is the denial of any risk through the show of self-confidence of the fraudsters to avoid getting caught. Self-confidence has the reinforcing effect as it encourages undecided individuals to engage in internet fraud. Our results show that internet fraudsters compare their crimes and are emboldened to commit internet fraud. For example, when an individual considers corruption as a form of extortion but believes society does not hold perpetrators accountable, then committing internet fraud such as credit card fraud may not be a costly crime. Thus, internet fraudsters do not consider those other crimes as different from what they do.

Our study reinforces the extensive use of comparing of risk as denial of risk technique by deviants in previous studies (Peretti-Watel 2003; Vida et al. 2012; Grabosky 2015). These internet fraudsters "see" other crimes such as, arm robbery, blood rituals, stealing from the Government as comparable to internet fraud and this perception helps them to rationalize their criminal behavior. Preventing internet fraud requires the global effort of all stakeholders including law enforcement agencies to confront it (Gottschalk and Smith 2011). The results of the study suggest that preventing internet fraud requires concerted effort to raise the level of risk associated with these crimes.

Future studies should attempt to understand how denial of risk compares with other techniques employed by individuals such as neutralization techniques who may want to commit an internet crime. Furthermore, researchers should seek to understand how age and technical experience play a role in the intention to commit internet crime.

Appendix

(See Table 3).

Table 3. Survey instrument

Item		Loading
Perceived scapegoating		
Dorsg1	Defrauding "clients" is not as bad as armed robbery	–
Dorsg2	Defrauding "clients" is not as bad as 'blood money'	0.829
Dorsg3	Defrauding "clients" is not as bad as 'Sakawa'	0.875
Dorsg4	Defrauding "clients" is not as bad as corruption	0.735
Perceived self-confidence		
Dorsc1	I feel confident in my ability to defraud "clients"	
Dorsc2	I know how to get "clients" believe in me than the average person	0.836
Dorsc3	It is not dangerous to maintain relationship with "clients" after defrauding them	0.858
Dorsc4	I have confidence in determining "clients" who are less willing to be defrauded	0.749
Perceived comparison-between-risk		
Dorcr1	Defrauding "clients" who is in relationship is no different from taking money from a spouse	–
Dorcr2	Defrauding "clients" is no different from begging for livelihood	0.813
Dorcr3	Defrauding "clients" is no different from paid workers who receive tips before they provide service	0.792
Dorcr4	Defrauding "clients" is not no different from taking money from a woman you are not sure you will marry	0.758
Intention to commit internet fraud		
Icifid1	What is the chance that you will defraud "clients"?	0.865
Icifid2	I am certain that I will defraud "clients"	0.859
Icifid3	I am likely to defraud "clients"	0.752
Icifidp1	I tell all my "clients" lies	0.785
Icifidp2	My "clients" believe the lies I tell them	0.863
Icifidp3	My "clients" don't know I am deceiving them	0.830
Icifidp4	I am crafty with my lies	0.746
Icifidp5	"Clients" needs to believe your story before you get the money	–

References

Apostolidis, T., Fieulaine, N., Simonin, L., Rolland, G.: Cannabis use, time perspective and risk perception: evidence of a moderating effect. Psychol. Health **21**(5), 571–592 (2006)

Boateng, R., Longe, O., Isabalija, R.S., Budu, J.: Sakawa - cybercrime and criminality in Ghana. J. Inf. Technol. Impact **11**(2), 85–100 (2011)

Boyle, K.M., Walker, L.S.: The neutralization and denial of sexual violence in college party subcultures. Deviant Behav. **37**(12), 1392–1410 (2016)

Brooks, G.: Explaining corruption: drifting in and out of corruption and techniques of neutralization. In: Criminology of Corruption, pp. 107–125. Palgrave Macmillan, London (2016)

Chatterjee, S., Kar, A.K., Dwivedi, Y.K., Kizgin, H.: Prevention of cybercrimes in smart cities of India: from a citizen's perspective. Inf. Technol. People (2018). https://doi.org/10.1108/ITP-05-2018-0251

Choo, K.K.R.: Cyber threat landscape faced by financial and insurance industry. Trends Issues Crime Crim. Justice **408**, 1 (2011)

Choudrie, J., Dwivedi, Y.K.: Investigating the research approaches for examining technology adoption issues. J. Res. Pract. **1**(1), 1 (2005). http://jrp.icaap.org/index.php/jrp/article/viewFile/4/7

Gottschalk, P., Smith, R.: Criminal entrepreneurship, white-collar criminality, and neutralization theory. J. Enterp. Commun.: People Places Glob. Econ. **5**(4), 300–308 (2011)

Grabosky, P.: Organized cybercrime and national security. In: Cybercrime Risks and Responses, pp. 67–80. Palgrave Macmillan, London (2015)

Harris, L.C., Dumas, A.: Online consumer misbehavior: an application of neutralization theory. Mark. Theory **9**(4), 379–402 (2009)

Hutchings, A.: Hacking and fraud: qualitative analysis of online offending and victimization. In: Global Criminology: Crime and Victimization in the Globalized Era, pp. 93–114 (2013)

Jegede, A.E., Olowookere, I.E., Elegbeleye, A.O.: Youth identity, peer influence and internet crime participation in Nigeria: a reflection. IFE Psycholog **24**(1), 37–47 (2016a)

Jegede, A.E., Oyesomi, K., Olorunyomi, B.R.: Youth crime and the organized attributes of cyber fraud in the modern technological age: a thematic review. Int. J. Soc. Sci. Hum. Rev. **6**(1), 153–164 (2016b)

Koay, K.Y.: Understanding consumers' purchase intention towards counterfeit luxury goods: an integrated model of neutralization techniques and perceived risk theory. Asia Pac. J. Mark. Logistics **30**(2), 495–516 (2018)

Kubic, T.T.: Internet Fraud Complaint Center (2001). https://archives.fbi.gov/archives/news/testimony/internet-fraud-crime-problems

Lazarus, S.: Birds of a feather flock together: the Nigerian cyber fraudsters (Yahoo Boys) and hip hop artists. Criminol. Crim. Justice Law Soc. **19**(2), 63–80 (2018)

Li, W., Cheng, L.: Effects of neutralization techniques and rational choice theory on internet abuse in the workplace. In: PACIS, p. 169 (2013)

McMullan, J.L., Rege, A.: Online crime and internet gambling. J. Gambl. Issues (24), 54–85 (2010)

Mekonnen, S., Padayachee, K., Meshesha, M.: A privacy preserving context-aware insider threat prediction and prevention model predicated on the components of the fraud diamond. In: 2015 Annual Global Online Conference on Information and Computer Technology (GOCICT), pp. 60–65. IEEE (2015)

Morris, R.G., Higgins, G.E.: Neutralizing potential and self-reported digital piracy: a multitheoretical exploration among college undergraduates. Crim. Justice Rev. **34**(2), 173–195 (2009)

Odou, P., Bonnin, G.: Consumers' neutralization strategies to counter normative pressure: the case of illegal downloading. Recherche et Applications en Marketing (English Edition), **29**(1), 103–121 (2014)

Park, J., Sung, C.: The effect of online piracy deterrence on self-control and piracy intention, PACIS, Jooyeon Park, School of Business, Yonsei University, Seoul, Korea (2015)

Peretti-Watel, P.: Neutralization theory and the denial of risk: some evidence from cannabis use among French adolescents*. Br. J. Sociol. **54**, 21–42 (2003)

Shareef, M.A., Dwivedi, Y.K., Kumar, V., Davies, G., Rana, N., Baabdullah, A.: Purchase intention in an electronic commerce environment: a trade-off between controlling measures and operational performance. Inf. Technol. People (2018). https://doi.org/10.1108/ITP-05-2018-0241

Sigala, M.: How "Bad" are you? Justification and normalisation of online deviant customer behaviour. In: Schegg, R., Stangl, B. (eds.) Information and Communication Technologies in Tourism 2017, pp. 607–622. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-51168-9_44

Siponen, M., Vance, A.: Neutralization: new insights into the problem of employee information systems security policy violations. MIS Q. **34**, 487–502 (2010)

Smith, W.R., Torstensson, M., Johansson, K.: Perceived risk and fear of crime: gender differences in contextual sensitivity. Int. Rev. Victimol. **8**(2), 159–181 (2001)

Sugiura, L.: Challenging the risks in online medicine purchasing: respectable deviance. In: Respectable Deviance and Purchasing Medicine Online, pp. 101–138. Palgrave Macmillan, Cham (2018)

Vida, I., Kos Koklič, M., Kukar-Kinney, M., Penz, E.: Predicting consumer digital piracy behavior: the role of rationalization and perceived consequences. J. Res. Interact. Mark. **6**(4), 298–313 (2012)