11-5-2020

The Restrictive Deterrent Effect of Warning Messages Sent to Active Romance Fraudsters: An Experimental Approach

Fangzhou Wang
Georgia State University

C. Jordan Howell
Georgia State University

David Maimon
Georgia State University

Scott Jacques
Georgia State University

The Restrictive Deterrent Effect of Warning Messages Sent to Active Romance Fraudsters: An Experimental Approach

Fangzhou Wang[1], C. Jordan Howell[1], David Maimon[1], Scott Jacques[2]

[1]Georgia State University, [2]Criminology Open and Georgia State University

Published on: Nov 05, 2020

DOI: 10.21428/cb6ab371.c6eae022

ABSTRACT

Victims of romance fraud experience both a financial and emotional burden. Although multiple studies have offered insight into the correlates of perpetration and victimization, no known study has examined if, and how, romance fraud can be curtailed. The current study uses a randomized experimental design to test the restrictive deterrent effect of warning messages sent to romance fraudsters via email. We find that active romance fraudsters who receive a deterrence message, instead of non-deterrence messages, respond at a lower rate; and, among those who respond, use fewer words and have a lower probability of seeking reply without denying wrongdoing. The results provide support for restrictive deterrence in cyberspace. Theoretical and policy implications are discussed.

INTRODUCTION

The internet provides myriad opportunities for people to commit crimes (Bossler & Berenblum, 2019). One type of crime is fraud, defined as an act in which the facts of exchange do not match the communication surrounding it (Jacques & Wright, 2008). Online fraud is the most frequently reported cybercrime, with the highest associated monetary loss (Internet Crime Report, 2019). Various forms of online fraud exist, including, but not limited to, business email compromise, phishing/spoofing, and advanced fee payment fraud (Internet Crime Report, 2019).

In this article, our focus is romance fraud. Romance fraud, compared to other form of fraud, is relatively new, and have a unique emotional component. They involve "cybercriminals pretending to initiate a relationship through online dating sites and then defrauding their victims of a large sum of money" (Whitty & Buchanan, 2012). This relationship can be sought via email or on a variety of websites and "apps," such as those specific to dating or more general (e.g., Facebook, Twitter, Instagram, Google Hangout) (Federal Trade Commission, 2019). Many romance fraudsters are motivated by money, with the goal being to increase income from victims (Whitty & Buchanan, 2012).

The frequency and seriousness of romance fraud are on the rise. Victim-reports surged from roughly six thousand in 2014 to more than nineteen thousand in 2019 (Internet Crime Complaint Center, 2019). For the same years, the annual loss increased from $87 million to around $475 million (Internet Crime Complaint Center, 2019). In 2019, the average loss was around $24,000, which is three times higher than other types of fraud (Internet Crime Report, 2019). The harm is not only financial. Victims also experience psychological distress upon learning that their relationship was never real, and that they fell for a scam that cost them money (see Whitty & Buchanan, 2016).

Despite the numbers, scant attention has been given to this phenomenon in the criminological literature (Buchanan & Whitty, 2014), and the majority of these studies employ a qualitative approach. Whitty and colleagues (Whitty & Buchanan, 2012; Sorell & Whitty, 2019; Whitty, 2018; Whitty 2015) have been instrumental in bringing attention to romance scams. They introduced a formal definition; highlight the scale and scope of the phenomenon; explore the scam's anatomy; present psychological characteristics of offenders and victims; and, describe the obstacles and aids associated with helping victims (Buchanan & Whitty, 2014; Whitty & Buchanan, 2012, 2016; Sorell & Whitty, 2019; Whitty, 2018; Whitty 2015, 2018).

A few attempts have been made to better understand romance fraud using quantitative approach. For example, Whitty and Futter (2019) asked a sample of 261 participants with experience on dating sites and/or social networking sites to distinguish between 20 genuine dating profiles and 20 known scammer profiles. They found that correct judgements were often made by participants who scored lower in romantic beliefs, higher in impulsivity, higher in considerations for future consequences, and had previously seen romance scams (Whitty & Futter, 2019). Suarez-Tangil and colleagues (2019) investigated the archetype of online dating profiles to develop a system for automatically detecting this type of fraud. Also, they analyzed conversations between victims and romance scammers to determine potential linguistic hints for identifying the initiation of romance scams.

No known study of romance fraud uses criminological theory to explain its occurrence and curtailment. One such theory is restrictive deterrence (Gibbs, 1975), rooted in the rational choice paradigm (Cornish & Clark, 1986). As its name suggest, restrictive deterrence theory contends that when offenders perceive the threat of sanction, be it formal or informal, they would limit the frequency or seriousness of their offenses (Gibbs, 1975). The efficacy of this theory has been demonstrated in the physical world and in cyberspace, using qualitative and experimental research (Jacobs, 1996a; Maimon et.al, 2014).

In cyberspace, restrictive deterrence has been found to explain trespassing, which requires a higher level of technical expertise (Maimon et.al, 2014). Unclear is whether that will hold true for less technical forms of cybercrime, such as romance fraud. This article addresses that lacuna and another one: whether a potential victim's style of communicating to a romance fraudster affects their response. Our method—a randomized experimental approach—overcomes a limitation of prior studies, namely the inability to make strong causal inferences. Before presenting and discussing our hypotheses, current study, and findings, we review the literature that informs this article.

LITERATURE REVIEW

Romance Fraud

As characterized by Whitty (2015), romance scams have five distinct stages, though all may not occur in any given (attempted) romantic fraud. The first stage involves baiting victims: fraudsters tend to use bogus profile pictures with low quality and attractive figures. After successfully getting a response from their targets, fraudsters initiate the second stage, grooming: fraudsters try to increase the intimacy of relationship to the point that victims are willing to send money. The third stage is the sting: fraudsters attempt to get money from their victims, typically by sharing a crisis story (e.g., bankruptcy, death of a parent. The fourth stage is sexual abuse. Here, the fraudsters' motivation is not money but to humiliate victims, ultimately, by asking them to perform sexual acts in front of a webcam. The last stage is the revelation: victims discover they have been defrauded and decide how to respond.

There is extensive research addressing the psychological influence that fraudsters, of all sorts, impose on potential victims. Rusch (2003) found that they majority of fraudsters use three main techniques to impact the beliefs and behaviors of their victims. Two of these techniques are pertinent to romance scams. One is a peripheral route of persuasion: romance fraudsters use statements intended to make potential victims susceptible to strong emotions (e.g., joy, fear), which interferes with their ability to engage in good decision-making (see also Langenderfer & Shimp, 2001). The second technique is an appeal to authority: fraudsters increase their legitimacy (e.g., by claiming to work for an important organizations) and thereby more effectively persuade victims. Loewenbstein (1996) also provides insight into the psychology of romance frauds via the concept of "visceral influence." This refers to factors that have "a direct hedonic impact" and "an effect on the relative desirability of different goods and actions" (p. 272). This concept is evident in that romance fraudsters create false identities that are very similar to those of targets. For example, they will claim to live in the same area as victims, prefer similar food, or belong to the same religion.

Restrictive Deterrence

Rooted in the concept of free will and utilitarian principles, the deterrence doctrine views people as rational. That is, they assess the benefits and costs of various lines of action, and do whichever is perceived to have the greatest utility (i.e., benefit minus costs). Deterrence theory is traced to classic works of crime and control, such as those of Hobbes (1968), Beccaria (1995), and Bentham (1789). It was on the verge of being discredited by social scientists, until reinvigorated by Becker (1968) and Gibbs (1968). Becker (1968) integrated economic/utility ideas into the criminal decision-making process. Gibbs (1968) provided an example of how to empirically test deterrence theory, namely by examining the relationship between the certainty and severity of punishments on individuals' offending.

Gibbs (1975) went further by differentiating "absolute deterrence" from "restrictive deterrence." The former refers to never committing a (particular) crime due to fear of sanction. Our focus is restrictive deterrence, or why offenders commit offenses in some situations but not others (see also Paternoster,

1989; Jacobs, 1996). Most research on restrictive deterrence is qualitative and focused on "analog" offenders and offenses, meaning those outside cyberspace. Example include drug dealers, burglars, auto thieves, carjackers, robbers and violent retaliators (e.g., Jacobs, 1993, 1996; Jacobs & Miller, 1998; Jacobs & Cherbonneau, 2014; Cherbonneau & Copes, 2006; Dickinson & Wright, 2015). All of this research shows that offenders have ways to reduce the overall risk that, by their very nature, entail committing fewer offenses. In other words, that have a restrictive deterrent effect.

A vein of deterrence research is concerned with warning messages. Geerken and Gove (1975) contend that warning messages are necessary and indispensable to preventing crime; and, for messages to be effective, they must be displayed to the target audience (Geerken & Goove, 1975). This idea harks back to Beccaria (1995), who wrote: "The more people understand the sacred code of the laws … the fewer will be crimes, for there is no doubt that ignorance and uncertainty of punishment" (p. 17).

Research testing the effect of warning messages shows mixed results. Some studies find that warning messages reduce offenses, such as theft (Solymosi et al., 2015), unsafe driving (Rama and Kulmala, 2000), and insurance fraud (Blais and Bacher, 2007). Other studies find that warning messages can have no effect (Green, 1985; Lowman, 1992; Decker, 1972) or even the opposite effect (Snyder & Blood, 1991; Grabosky, 1996).

For cybercrime, there is less research on warning messages as restrictive deterrents, but the findings point to a crime reduction effect. In a series of studies, Maimon and colleagues (Howell et al., 2017; Maimon et al., 2014; Testa et al., 2017; Wilson et al., 2015) found that after hackers infiltrate a computer system, they reduce their illicit behavior post receipt of a warning message. That body of work uses "honeypots," which are somewhat like (non-lethal) mouse or bug traps in which offenders are lured into a space to observe their behavior. Those studies are limited in that, one, they are focused on hacking and, two, that honeypot-based data suffer from notable limitations (Bossler, 2017). Moreover, they are not necessarily generalizable to other forms of cybercrime (Bossler, 2017). It is unknown whether similar results will be found for other cybercrimes other data collection techniques.

CURRENT STUDY

We examine whether deterrent messages sent to active romance fraudsters have a restrictive deterrent effect. To test the effect of deterrence messages on the initiation and extent of romance fraud, we formed two hypotheses and tested them with an experiment, described in the next section. We hypothesize: Romance fraudsters who receive a deterrence message, instead of non-deterrence messages, (H1) respond at a lower rate; and, (H2) among those who respond, use fewer words in their immediate responses. After testing those hypotheses, we turn to an exploratory analysis that uses mixed-methods to shed light on the manner of engagement by romance fraudsters. Based on our analysis of qualitative responses, we formed a third hypothesis for testing: (H3) Romance fraudsters

who receive and respond to a deterrence messages, instead of non-deterrence messages, have a lower probability of seeking a reply without denying wrongdoing.

METHOD

The following procedure was approved by our university's Institutional Review Board (IRB). An initial step in data collection was gathering a list of active romance fraudsters' email addresses. We did so using a public online dating scam list, maintained by stop-scammers.com. *This website uses victims' reports to expose offenders and build awareness. Information on the site includes the offenders' age,* gender, address, email address, phone number, and social media information. This information is what offenders provide to their victim, so it represents their scamming identities, not necessarily their real ones. Note that the website only includes information for scammers who claim to be female.

The site has a rigorous vetting process. It requires victims to provide the administrators documented evidence of the attempted romance scam. We confirmed the validity of the site's process by reporting a fictional romance fraud attempt to it, which was rejected due to sufficient evidence. Though anecdotal, the rejection of this fictional report, coupled with the website's reputation, gives us confidence that the persons we messaged are in fact romance fraudsters. What we do not know is whether two or more email addresses are controlled by the same real individual. Yet for the sake of not writing in a pedantic and awkward language, we refer to each email address as a distinct individual/participant.

Next, we used a python scraper to gather the email addresses of all romance fraudsters reported to the site in 2019, the most recent year of fully available data at the time of data collection. That is our temporal focus because we assume that those offenders, compared to those reported in prior years, are more likely to be *active* romance fraudsters (i.e., less likely to have desisted). That scrapping led us to obtain 546 unique email addresses. Our IRB prohibited us from gathering demographic information on the sample. That is not ideal, but not problematic given our focus and that the information has unknown validity (i.e., the reported traits may not match the offenders' actual traits).

To ensure endogeneity, the 546 email addresses were randomly assigned into three groups, the names of which reflect the tone of our emails to them: deterrent group (N = 182); promising group (N = 175); and, ambiguous group (N = 189). The deterrent group received the message: "I know you are scamming innocent people. My friend was recently arrested for the same offense and is facing 5 years in prison. You should stop before you face the same fate." The promising group was sent the message, "Hey, I saw your pictures. Can I send you money for a flight to visit me next week?" The ambiguous was sent a message that simply read "Hey."

These messages were automatically sent on February 20, 2020, at the same time, using a program developed in Python. Not all fraudsters received the automated message. In the deterrent group, 43

messages failed to send; the promising group, 47 messages; in the ambiguous group, 51 messages. This reduced our sample of email addresses for analysis from a total of 546 to 405, with 139 in the deterrent group, 129 in the promising group, and 138 in the ambiguous group. After sending the messages, we gathered data for the 405 persons until the end of March 20, 2020.

Our independent variable is *Deterrence*, which is coded as a dichotomous variable. Those who received a deterrence message (i.e., individuals assigned to deterrent group) receive a score of 1; otherwise, received a score of 0. We created three unique dependent variables to assess our hypotheses. The first variable, *Respond*, is coded as 1 if the fraudster responded to our message, and 0 if not. The second variable, *Words*, is simply a count of the number of words included in the immediate responses sent to us by the romance fraudsters. The last variable, *Seeking Reply Without Denial*, is coded as 1 if the person's words are meant to generate a reply but do not deny wrongdoing; otherwise, as 0.

We analyze the data in a stepwise fashion. First, descriptive statistics are calculated. Then, to test our first hypothesis, we employ a chi-square test of independence, followed by a robustness test to validate our findings. Next, to test our second hypothesis, we employ an independent sample t-test. Also, we employ an Anova test followed by a Tukey Pairwise Comparison test to determine which pair of means differ. To test our third hypothesis, we again employ a chi-square test of independence, followed by an additional robustness test to validate our findings. We are able to employ these simple models without controls due to the randomized nature of our field experiment; it ensures group equality on all observed and unobserved variables.

RESULTS

Descriptive statistics are reported in Table 1. Sixteen percent of participants responded to our message. The average number of words included in the response is 7.88, with a minimum of 0 words (no response) and maximum of 529 words. Among those who replied to our messages, 78% percent sought a reply from us. Results demonstrate variability in our dependent variable of interest.

Hypothesis 1

[INSERT TABLE 1 ABOUT HERE]

To examine group differences in response probability, we conducted a chi-square test of independence. Results are presented in Table 2. Recall that our first hypothesis is that romance fraudsters who receive deterrence messages, instead of non-deterrence messages, will respond at a lower rate. Our findings support this hypothesis. There is significant difference in the response rate between those who received a deterrent message and those who received non-deterrent messages, $x^2 = 7.04$, $p = 0.008$. Romance fraudsters who received the deterrence message had a response rate of 9%, whereas that of persons who received the other messages was 20%.

[INSERT TABLE 2 ABOUT HERE]

From the analysis presented in Table 2, it is unclear if the two non-deterrent messages skewed the results. Therefore, we separately examine each of the three groups using a chi-square test of independence. Results indicate there are significant differences in the response rate between the three groups, $x^2 = 8.03$, $p = 0.018$. Whereas romance fraudsters who received the deterrent message only responded 9% of the time, those who were messaged "Hi" replied at a rate of 17%; those who were sent the promising message replied at a rate of 22%. Again, this finding supports our first hypothesis.

Hypothesis 2

[INSERT TABLE 3 ABOUT HERE]

Recall our second hypothesis is that among persons who respond to us, those who receive the deterrent message, instead of non-deterrence messages, will use fewer words in the immediate responses. We tested this hypothesis using an independent sample T-test. It examined the mean difference in the number of words used in the immediate responses to the deterrent and non-deterrent messages. As presented in Table 4, we found that persons who were sent the deterrent message responded with 1.8 words on average, compared to 11 words among persons sent the non-deterrent messages. This finding is in the anticipated direction, and marginally significant ($t = 1.91$, $p = 0.06$), thus providing support for our second hypothesis.

[INSERT TABLE 4 ABOUT HERE]

Here too, however, that findings could be skewed by differences the groups who received the non-deterrent messages. Therefore, we examined mean differences among the three groups using Anova. The results remain marginally significant, $F = 2.65$, $p = 0.07$. As presented in Table 5, we found that persons who were sent the deterrent message responded with 1.8 words on average, compared to 14.8 words among persons sent the promising message, and 7.6 words among those sent the ambiguous message.

[INSERT TABLE 5 ABOUT HERE]

Using an Anova alone, it is impossible to determine which pair of means differ. Therefore, we turned to the Tukey Pairwise Comparison test, which is a post-hoc test used in analysis of variance. Results reported in table 6 show there is not a statistically significant difference in the number of words used in the immediate responses between the deterrent message group and the ambiguous group ($p = 0.56$), or between the latter and the group that received the promising message ($p = 0.41$). We do, though, observe a marginally significant difference in the mean number of words used between the deterrent and promising group ($p = 0.06$), indicating that the marginally significant results (see Tables 4 and 5)

are driven by differences between the groups that received the deterrent message and the promising message.

[INSERT TABLE 6 ABOUT HERE]

Exploratory Analysis

To better understand our data and, by extension, romance fraudsters, we conducted an exploratory analysis of responses. Recall that 65 persons replied to our messages. First, we qualitatively coded each person's textual message. These data are not large (~3,500 words), so we analyzed this content within a Microsoft Word document, rather than use a qualitative software package (e.g., NVivo).

We organized qualitative data into relatively unambiguous themes, or categories, reflective of our research foci. The most important emergent themes are *unambiguous denial* and a *desire to continue interaction*. The first of those was less prominent. Across the 65 responses, it was evident in 7 (11%) cases. This sort of reply was only sent by persons in the deterrent group. We received a total of 13 responses from people in this group, so a little more than half of them replied with unambiguous denial. Here are unedited examples:

> **Deterrence Group, Respondent 2:** I see you are joking.
>
> **Deterrence Group, Respondent 3:** Hello! I think you just wrote the wrong person This email was hacked several months ago and I'm glad I got it back so whatever has been done with this email I'm not liable for any damage and I'm sorry if you fell victim one way or the other. Lately I've been getting strange mails from strange people and it's really annoying. I already made a report so and you can do the same as well.
>
> **Deterrence Group, Respondent 9:** Hu, I am not a scammer.
>
> **Deterrence Group, Respondent 13:** I do not know who are you and where you get my mail... I do not understand your intentions and "warnings"! But i know for 100% that i can put you in prison for defamation! So, watch your words and have a happy life!

The additional three denials also display the more prominent theme across cases, namely a desire to continue interaction. The responders request more information about the accusation, which they deny:

> **Deterrence Group, Respondent 4:** HHello oh I'm very happy to see your letter !!! My mood is right up !!! Honey ... what are you talking about ??? I wrote to you to meet you dear! But what have I done wrong to you ??

> **Deterrence Group, Respondent 6:** Hello! I don't know who you are, and why you decided that I was deceiving someone! What do you want from me, and where did you get my email address?
>
> **Deterrence Group, Respondent 8:** What? Do you think I am scamming people? No wrong. It's more like I'm being scammed.

The other responses that seek further communication do not explicitly deny wrongdoing. These were found across members from all three groups. The responses often posed requests for more information about the sender, either in the form of a question or statement:

> **Ambiguous Group, Respondent 2:** I wish to get to know you. I am new to social networks. And I was at dating agency. The agency gave me your email. Now I will tell you a little about myself. My name is Anna. I am38 years old. I am from Russia. I've never been married, and I have no children. At the moment, I feel lonely. I really want to have a serious relationship. I want to get know you better. I hope you do not forget to write me.
>
> **Ambiguous Group, Respondent 3:** Hello who are you[?]
>
> **Ambiguous Group, Respondent 11:** Hi, I am live this site u come fast
>
> **Ambiguous Group, Respondent 19:** Hi, how are you doing today?
>
> **Deterrence Group, Respondent 1:** who is this please?
>
> **Deterrence Group, Respondent 7:** what are you talking about?
>
> **Promising Group, Respondent 4:** You saw my pictures where?
>
> **Promising Group, Respondent 5:** Of course, you can! Happy Weekend. Drop me a number I can text you on. Cheers. Angela
>
> **Promising Group, Respondent 12:** Hi, Do we know each other?

The other major theme is, in some respects, not a theme at all: ambiguous responses. Seven replies were coded as such, accounting for 11% of all replies. In the deterrent group, respondent 2 wrote "you crying." In the ambiguous group, respondent 25 replied "lol funny." And in the ambiguous, which recall received the "Hi" message, 5 respondents (#s 4, 13, 15, 23, and 24) replied with "Hi," "Hey," or "HEY." Though something like "hi" is plausibly interpretable as seeking further interaction, it is more conservative to code as ambiguous.

Hypothesis 3

Finally, we used our qualitative findings to construct a final hypothesis suitable for testing: Romance fraudsters who receive and respond to a deterrence messages, instead of non-deterrence messages, have a lower probability of seeking a reply without denying wrongdoing.

We conducted a chi-square test of independence. Results, as presented in Table 7, demonstrate that fraudsters who receive a deterrent message are less likely to do so, x2 = 15.39, p = 0.000. Specifically, 38% of those who received the deterrent message sought a reply without denying wrongdoing in comparison to 88% of those who received other types of messages. Thus, we find support for the hypothesis.

[INSERT TABLE 7 ABOUT HERE]

From the analysis presented in Table 7, it is unclear if the two non-deterrent messages skewed the results. Therefore, we again separately examine each of the three groups using a chi-square test of independence. Results indicate there are significant differences in the rate of seeking reply between the three groups, x^2 =17.66, p = 0.000. Whereas romance fraudsters who received the deterrent message only sought a reply without denying wrongdoing 38% of the time, those who received the ambiguous message did so at a rate of 79%, and those who were sent the promising message at a rate of 96%. Again, this finding supports our third hypothesis.

[INSERT TABLE 8 ABOUT HERE]

DISCUSSION AND CONCLUSION

Cybercrime will continue to increase as society becomes more reliant on computers and networked devices. Thus, so too will romance fraud. Research has examined its impact on victims and detailed its methods of execution. Less scholarship focuses on whether, and how, to mitigate romance fraud. To build an evidence-base in this area, we tested three hypotheses: Romance fraudsters who receive a deterrence message, instead of non-deterrence messages, (H1) respond at a lower rate; (H2) among those who respond, use fewer words in their immediate responses, and (H3) less often seek a reply without denying wrongdoing.

Our results show that romance fraudsters can be restrictively deterred (Gibbs, 1975; Jacobs, 1996). In other words, threatening them with sanction leads them to reduce the extent of their offending. We found that romance fraudsters who were sent a deterrence message, instead of a promising or ambiguous message, less often replied; used fewer words in their replies; and, less often replied without denying wrongdoing. Those findings lend support to the validity of restrictive deterrent theory. Our study also serves as an example of how to test restrictive deterrence in cyberspace. To our knowledge, this is the first study to directly send deterrence cues to active offenders and examine

their responses. In doing so, we present additional evidence that cyber-offenders are rational decision-makers.

Furthermore, the results speak to the utility of a proactive approach to mitigating romance fraud, and cybercrime more broadly. It is clear that once they are committed, law enforcement agencies are largely unable to do much about them (Burruss et.al, 2019). It is rational, then, to reallocate resources from responding to preventing cybercrimes. Our findings add to the growing evidence-based for deterring and otherwise nudging offenders, analog and cyber, to commit fewer and lesser serious offenses (Maimon et.al, 2014). How to take advantage of this effect is an open question. With respect to romance fraud, the purveyors of dating platforms could develop an algorithm that identifies the likely offenders, and then send them automated but realistic deterrence messages, lest they pass a screening protocol. Potentially, that approach could be used with other fraudsters, too, such as those involved in the sale of counterfeit goods.

The results and their implications should be considered in light of our study's limitations, which future research should address. The first issue was mentioned in the method section: We do not know if two or more email addresses are controlled by the same real individual. To the extent that is the case, the validity of our findings is undermined due to contamination. Second, some of the email addresses that we messaged may have been inappropriately listed on the website that we used to collect them, which would undermine the validity of our findings. The same could also result if, third, romance fraudsters rarely receive messages like those we sent. Fourth, and finally, the generalizability of our results is unknown. For instance, the results may not apply to male personas, as the website we used to obtain email addresses was limited to female personas. Likewise, it is unknown whether and how the results would differ for research using different messages, websites or apps.

In conclusion, and the limitations notwithstanding, this article has shown that deterrent messages alter the behavior of online romance fraudsters. As such, the findings support and expand on the restrictive deterrence perspective (Gibbs, 1975), while providing a potential avenue for proactive mitigation strategies. We also provide additional evidence supporting the assumption of rationality and decision-making among cyber-offenders. As time progresses, technological advancements continually change the cyber landscape. Human behavior, however, remains constant. Therefore, to ensure a safer cyberspace requires research into the human-factor in cybercrime.

REFERENCES

Ariel, Barak. 2012. Deterrence and moral persuasion effects on corporate tax compliance: Findings from a randomized control trial. *Criminology* 50:27–69.

Armstrong, R. A. (2014). When to use the B onferroni correction. *Ophthalmic and Physiological Optics*, *34*(5), 502-508.

Arias-Carrión, Ó., & Pöppel, E. (2007). Dopamine, learning, and reward-seeking behavior. *Acta neurobiologiae experimentalis*.

Beccaria, C. (1764). On crimes and punishments. *Criminology Theory: Selected Classic Readings*, 367.

Becker, G. S. (1968). Crime and punishment: An economic approach. In *The economic dimensions of crime* (pp. 13-68). Palgrave Macmillan, London.

Bentham, J. (1789). *An introduction to the principles of morals and legislation: printed in the year 1780, and now first published*. T. Payne.

Blais, Etienne, and Jean-Luc Bacher. 2007. Situational deterrence and claim padding: Results from a randomized field experiment. *Journal of Experimental Criminology* 3:337–52.

Bossler, A. M. (2017). Need for debate on the implications of honeypot data for restrictive deterrence policies in cyberspace. *Criminology & Pub. Pol'y*, *16*, 679.

Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research.

Brantingham, P. J., & Brantingham, P. (2001). The implications of the criminal event model for crime prevention. *The process and structure of crime: Criminal events and crime analysis*, *9*, 227-303.

Briar, S., & Piliavin, I. (1965). Delinquency, situational inducements, and commitment to conformity. *Soc. Probs.*, *13*, 35.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261-283.

Burruss, G., Howell, C. J., Bossler, A., & Holt, T. J. (2019). Self-perceptions of English and Welsh constables and sergeants preparedness for online crime. *Policing: An International Journal*.

Cherbonneau, M., & Copes, H. (2006). 'Drive it like you Stole it' Auto Theft and the Illusion of Normalcy. *British Journal of Criminology*, *46*(2), 193-211.

Clark, R. V. (1997). Situational crime prevention. *Successful Case Studies, Harrow and Heston Publishers, 2th Edition, Guilderland, New York*.

Coleman, Stephen (2007). *The Minnesota Income Tax Compliance Experiment: Replication of the Social Norms Experiment*. http://ssrn.com.

Cornish D, Clark, Rv. (1986). The Reasoning Criminal: Rational choice Perspectives on Offending. New York: Springer-Verlag.

Cusson, Maurice. (1993) Situational deterrence: Fear during the criminal event. In *Crime Prevention Studies*, Vol. 1, ed. Ronald V. Clarke. Monsey, NY: Criminal Justice Press.

Decker, John F (1972). Curbside deterrence? An analysis of the effect of a slug-rejecter device, coin-view window and warning labels on slug usage in New York City parking meters. *Criminology* 10:127–42.

Dickinson, T., & Wright, R. (2015). Gossip, decision-making and deterrence in drug markets. *British Journal of Criminology*, *55*(6), 1263-1281.

Federal Bureau of Investigation: Internet Crime Complaint Center (2019), *2019 Internet Crime Report*. Retrieved from https://pdf.ic3.gov/2019_IC3Report.pdf.

Geerken, M. R., & Gove, W. R. (1975). Deterrence: Some theoretical considerations. *Law & Society Review*, *9*(3), 497-513.

Gibbs, J. P. (1968). Crime, punishment, and deterrence. *The Southwestern Social Science Quarterly*, 515-530.

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

Goette, L., & Stutzer, A. (2020). Blood donations and incentives: Evidence from a field experiment. *Journal of Economic Behavior & Organization*.

Goffman, E. (1955). On face-work: An analysis of ritual elements in social interaction. *Psychiatry*, *18*(3), 213-231.

Goldstein, N. J., Cialdini, R. B., & Griskevicius, V. (2008). A room with a viewpoint: Using social norms to motivate environmental conservation in hotels. *Journal of consumer Research*, *35*(3), 472-482.

Green, Gary S. 1985. General deterrence and television cable crime: A field experiment in social control. *Criminology* 23:629–45.

Grabosky, P. N. (1996). Unintended consequences of crime prevention. Crime Prevention Studies, 5(1), 25-56.

Hobbes, Thomas, 1588-1679. (1968). Leviathan. Baltimore: Penguin Books.

Howell, C. J., Cochran, J. K., Powers, R. A., Maimon, D., & Jones, H. M. (2017). System Trespasser Behavior after Exposure to Warning Messages at a Chinese Computer Network: An

Examination. *International Journal of Cyber Criminology*, *11*(1).

Internet Crime Report (2019). Internet Crime Complaint Center. Retrieved from https://pdf.ic3.gov/2019_IC3Report.pdf.

Jacobs, B. A. (1993). Undercover deception clues: A case of restrictive deterrence. *Criminology*, *31*(2), 281-299.

Jacobs, B. A. (1996a). Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence. *Justice Quarterly*, *13*(3), 359-381.

Jacobs, Bruce A. (1996b). Crack dealers and restrictive deterrence: Identifying narcs. *Criminology* 34:409–431.

Jacobs, B. A., & Miller, J. (1998). Crack dealing, gender, and arrest avoidance. *Social Problems*, *45*(4), 550-569.

Jacobs, Bruce A. (2010). Deterrence and deterrability. *Criminology* 48:417–41.

Jacobs, B. A., & Cherbonneau, M. (2014). Auto theft and restrictive deterrence. *Justice quarterly*, *31*(2), 344-367.

Jacobs, B. A., & Cherbonneau, M. (2014). Auto theft and restrictive deterrence. *Justice quarterly*, *31*(2), 344-367.

James, J. M., & Bolstein, R. (1990). The effect of monetary incentives and follow-up mailings on the response rate and response quality in mail surveys. *Public opinion quarterly*, *54*(3), 346-361.

Jones, H. M. (2014). *The restrictive deterrent effect of warning messages on the behavior of computer system trespassers* (Doctoral dissertation).

Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles. *International Journal of Cyber Criminology*, *9*(2).

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, *18*(7), 763-783.

Larson, P. D., & Chow, G. (2003). Total cost/response rate trade-offs in mail survey research: impact of follow-up mailings and monetary incentives. *Industrial Marketing Management*, *32*(7), 533-537.

Lea, S.E.G. Fischer, P. and Evans, K.M. (2009), "The psychology of scams: provoking and committing errors of judgement, report for the office of fair trading", retrieved from https://ore.exeter.ac.uk/repository/handle/10871/20958.

Lowman, J. (1992). Street prostitution control some Canadian reflections on the Finsbury Park experience. British Journal of Criminology, 32(1), 1-17.

Loewenstein, G. (1996). Out of control: Visceral influences on behavior. *Organizational behavior and human decision processes*, *65*(3), 272-292.

Luu, V., Land, L., & Chin, W. (2017). Safeguarding Against Romance Scams–Using Protection Motivation Theory.

Lynch, H. F., Joffe, S., Thirumurthy, H., Xie, D., & Largent, E. A. (2019). Association between financial incentives and participant deception about study eligibility. *JAMA network open*, *2*(1), e187355-e187355.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33-59.

Maimon, D., Santos, M., & Park, Y. (2019). Online deception and situations conducive to the progression of non-payment fraud. *Journal of Crime and Justice*, *42*(5), 516-535.

Meier, R. F., Kennedy, L. W., & Sacco, V. F. (Eds.). (2001). *The process and structure of crime: Criminal events and crime analysis* (Vol. 9). Transaction Publishers.

Nederhof, A. J. (1983). The effects of material incentives in mail surveys: Two studies. *Public Opinion Quarterly*, *47*(1), 103-112.

Osgood, D. W. (2000). Poisson-based regression analysis of aggregate crime rates. *Journal of quantitative criminology*, *16*(1), 21-43.

Paternoster, R. (1989). Absolute and restrictive deterrence in a panel of youth: Explaining the onset, persistence/desistance, and frequency of delinquent offending. *Social Problems*, *36*(3), 289-309.

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., & Madensen, T. D. (2006). The Empirical Status of Deterrence Theory: A Meta-Analysis.

Rama, Pirkko, and Risto Kulmala (2000). Effects of variable message signs for slippery road conditions on driving speed and headways. *Transportation Research* 3:85–94.

Rusch, J. J. (1999, June). The "social engineering" of internet fraud. In *Internet Society Annual Conference, http://www. isoc. org/isoc/conferences/inet/99/proceedings/3g/3g_2. htm*.

Serin, R. C., & Hanby, L. J. (2009). *Offender Incentives and Behavioural Management Strategies*. Ottawa: Correctional Service of Canada.

Schultz, Wesley P., and Jennifer J. Tabanico (2009). Criminal beware: A social norms per- spective on posting public warning signs. *Criminology* 47:1201–22.

Shaari, A. H., Kamaluddin, M. R., Paizi, W. F., & Mohd, M. (2019). Online-Dating Romance Scam in Malaysia: An Analysis of Online Conversations between Scammers and Victims. *GEMA Online® Journal of Language Studies*, *19*(1).

Shihadeh, E. S., & Nedd, A. N. (1973). Inmate evaluation of a penitentiary incentive program. *Canadian Journal of Criminology and Corrections*, *15*(4), 229-238.

Short Jr, J. F. (1998). The level of explanation problem revisited—The American Society of Criminology 1997 presidential address. *Criminology*, *36*(1), 3-36.

Snyder, L. B., & Blood, D. J. (1992). Caution: Alcohol advertising and the Surgeon General's alcohol warnings may have adverse effects on young adults. *Journal of Applied Communication Research*, *20*(1), 37-53.

Solymosi, R., Borrion, H., & Fujiyama, T. (2015). Crowd Spatial Patterns at Bus Stops: Security Implications and Effects of Warning Messages. In *Safety and Security in Transit Environments* (pp. 156-178). Palgrave Macmillan, London.

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. *Security Journal*, *32*(3), 342-361.

Stark, R. (1987). Deviant places: A theory of the ecology of crime. *Criminology*, *25*(4), 893-910.

Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2019). Automatically dismantling online dating fraud. *IEEE Transactions on Information Forensics and Security*, *15*, 1128-1137.

Testa, A., Maimon, D., Sobesto, B., & Cukier, M. (2017). Illegal roaming and file manipulation on target computers: Assessing the effect of sanction threats on system trespassers' online behaviors. *Criminology & Public Policy*, *16*(3), 689-726.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181-183.

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, *53*(4), 665-684.

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443-455.

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176-194.

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behavior, and social networking*, *21*(2), 105-109.

Whitty, M. T., & Futter, A. (2019). Who can spot an online romance scam? *Journal of Financial Crime*.

Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The effect of a surveillance banner in an attacked computer system: Additional evidence for the relevance of restrictive deterrence in cyberspace. *Journal of Research in Crime and Delinquency*, *52*(6), 829-855.

TABLES

Tables.docx 45 KB