Copyright © 2020 International Journal of Cyber Criminology – ISSN: 0974–2891
January - June 2021. Vol. 15(1): 1–16. DOI: 10.5281/zenodo.4766529
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

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

Fangzhou Wang[1]
Georgia State University

C. Jordan Howell[2]
The University of Texas at El Paso

David Maimon[1], **Scott Jacques**[1]
Georgia State University

Abstract

Romance scams occur when a fraudster adopts a fake online identity to gain a victim's affection and trust and uses the illusion of a romantic or close relationship, eventually to steal money from the victim. Victims of such romance fraud experience suffer both 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 used a randomized experimental design to test the restrictive deterrent effect of warning messages sent to romance fraudsters via email. The sample consisted of 405 active email addresses, distributed among three groups: deterrent group, promising group, and ambiguous group. Using the mixed research design, the independent variable was Deterrence; while the dependent variables were Responses, words used by respondents and Seeking Reply Without Denial. The data was analyzed in a stepwise fashion through descriptive statistics, a chi-square test of independence, ANOVA test followed by a tukey kramer pairwise comparison test. The findings revealed that active romance fraudsters who received a deterrence message, instead of non-deterrence messages, responded at a lower rate; and, among those who responded, they used fewer words and had a lower probability of seeking reply without denying wrongdoing. The results provide support for restrictive deterrence in cyberspace. Theoretical and policy implications have also been discussed.

Keywords – Cybercrime, Cybersecurity, Online Fraud, Restrictive Deterrence, Romance Fraud

[1] Department of Criminal Justice and Criminology, Georgia State University
[2] Department of Criminal Justice, The University of Texas at El Paso

Introduction

A new era has begun of malicious cyber activities threatening both public safety and a country's economic security. Nations strategize to curb these cybercrimes by not only imposing consequences against the cyber criminals but also to equip the Internet with stronger capabilities. The internet has provided myriad opportunities for people to commit crimes (Bossler & Berenblum, 2019), including the online 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 Complaint Center, 2019). Various forms of online fraud exist, including, but not limited to, business email compromise, phishing/spoofing, and advanced fee payment fraud (Internet Crime Complaint Center, 2019; Maimon, Howell, Perkins, et al., 2021).

In this study, the focus is on Romance fraud which, compared to other forms of fraud, is relatively new and has a unique emotional component (C. Cross, 2020). It involves "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 by victimizing others (Whitty & Buchanan, 2012).

The frequency and seriousness of romance fraud are on the rise. Victim-reports (in the United States) have 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 reported in the United States 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 Complaint Center, 2019). The harm is not only financial. Victims also experienced psychological distress upon learning that their relationship was never real, and that they fell for a scam that cost them money (Cassandra Cross et al., 2018). In fact, many victims reported the emotional burden to be harder to cope with than the loss of money (C. Cross, 2020).

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

A few attempts have also been made to better understand romance fraud using a quantitative approach. For example, Whitty (2019) asked a sample of 261 participants about their 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, 2019). Suarez-Tangil et al. (2019) investigated the archetype of online dating profiles to develop a system for automatically detecting this type of fraud. They also 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 has so far used criminological theory to explain its occurrence and curtailment. A theory closer to its application is restrictive deterrence (J. P. Gibbs, 1975), rooted in the rational choice paradigm (Cornish & Clarke, 1986). As its name suggests, 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 (J. P. Gibbs, 1975). The efficacy of this theory has been demonstrated in the physical world and in cyberspace, using qualitative and experimental researches (Jacobs, 1996a; Maimon et al., 2014). In cyberspace, restrictive deterrence has been tested through the deliverance of warning messages. For instance, Maimon, Howell, Perkins, et al. (2021) found that messages warning malicious hackers of law enforcement operations reduce the proportion, frequency, and severity of their reoffending behaviors.

Although restrictive deterrence has been found to explain technical forms of cyber offending such as hacking (Maimon et al., 2014; Maimon, Howell, & Burruss, 2021), it is unclear whether this remains true for explaining less technical forms of cybercrime, such as romance fraud. Determining if, and how, romance fraud can be prevented is essential to the development of cyber-criminological theory and evidence-based policy initiatives. Thus, the current study seeks to determine if, and how, the content of messages delivered directly to active romance fraudsters alters their behavioral patterns. Our method—a randomized experimental approach—overcomes a limitation of prior studies, namely the inability to make strong causal inferences (C. Jordan Howell & Burruss, 2020). Before presenting and discussing this study's hypotheses and findings, we reviewed the literature that was referred to build this study.

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 the 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 are extensive research studies addressing the psychological influence that fraudsters, of all sorts, impose on potential victims. Rusch (1999) found that most 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 and Shimp (2001); Maimon et al. (2020)). These statements vary based on the type of fraud being committed. Although some scammers may offer monetary incentives, romance fraudsters spark the emotional state of joy with compliments of appearance and promises of love. The second technique is an appeal to authority: fraudsters increase their legitimacy (e.g., using Military identities) and thereby more effectively persuade victims (Cassandra Cross & Holt, 2021; Dieko, 2020). Loewenstein (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

Deterrence theory is traced to classic works of crime and control, such as those of Bentham (1789), Hobbes (1969), and Beccaria (1995). It was on the verge of being discredited by social scientists, until reinvigorated by Becker (2000) and Jack P Gibbs (1968). Becker (2000) integrated economic/utility ideas into the criminal decision-making process. Jack P 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. J. P. 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 while restrictive deterrence studies why offenders commit offenses in some situations but not others (see also Jacobs (1996a); Paternoster (1989)).

Most research on restrictive deterrence is qualitative and focuses on "analog" offenders and offenses, meaning those outside the cyberspace. Examples include drug dealers, burglars, auto thieves, carjackers, robbers and violent retaliators (e.g., Cherbonneau and Copes (2006); Dickinson and Wright (2015); Jacobs (1993, 1996b); Jacobs and Cherbonneau (2014); Jacobs and Miller (1998)). 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 also concerned with warning messages. Geerken and Gove (1974) 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 & Gove, 1974; Smith & Stamatakis, 2020). 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 (Bassey, 2020; Solymosi et al., 2015), unsafe driving (Rämä & Kulmala, 2000), and insurance fraud (Blais & Bacher, 2007; Kashif & Akhtar, 2020). Other studies find that warning messages can have no effect (Decker, 1972; Green, 1985; Lowman, 1992) or even the opposite effect (Grabosky, 1996; Snyder & Blood, 1992).

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 (Christian J 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 (Perkins & Howell, 2021). Those studies are limited since they focus on hacking or the honeypot-based data suffer from notable limitations (Bossler, 2017). Moreover, they are not necessarily generalizable to other forms of cybercrime (Bossler, 2017; Perkins & Howell, 2021). Although a recently published manuscript corroborated these findings using non-honeypot data (Maimon, Howell, & Burruss, 2021), the study also focused on a subset of the hacking community. Thus, it is still unknown whether similar results will be found for other, less technical, cybercrimes.

Rooted in the concept of free will and utilitarian principles, the deterrence doctrine views people as rational. They assess the benefits and costs of various lines of action and do whatever is perceived to have the greatest utility (i.e., benefit minus costs). It is therefore necessary to examine whether deterrent messages sent to active romance fraudsters have a restrictive deterrent effect. In order to test the effect of deterrence messages on the initiation and extent of romance fraud, two hypotheses were formed and tested with an experiment. The first hypothesis stated: Romance fraudsters who receive a deterrence message, instead of non-deterrence messages respond at a lower rate (H1); the second hypothesis stated (H1) that among those who respond, they use fewer words in their immediate responses (H2). After testing these hypotheses, an exploratory analysis was carried out through a mixed-method research design, to shed light on the manner of engagement by romance fraudsters. Based on the analysis of qualitative responses, a third hypothesis was formed for testing: Romance fraudsters who receive and respond to deterrence messages, instead of non-deterrence messages, have a lower probability of seeking a reply without denying wrongdoing (H3).

Methods

This research followed the procedure approved by our university's Institutional Review Board. In this procedure, the initial step was data collection involving gathering a list of active romance fraudsters' email addresses. This was done by using a public online dating scam list, maintained by stop-scammers.com. *This website uses victims' reports to expose offenders and build awareness. A wide range of information was available on the site, including the offenders' age,* gender, address, email address, phone number, and social media information. This information was what offenders provided to their victims, so it represented their scamming identities, not necessarily their real ones. It should be noted that the website only included information for scammers who claimed to be females.

The website used a rigorous vetting process. It required victims to provide the administrators the documented evidence of the attempted romance scam. The validity of the website's process was confirmed by reporting a fictional romance fraud attempt, which was rejected due to insufficient evidence. Though anecdotal, the rejection of this fictional report, coupled with the website's reputation, gave us confidence that the individuals we messaged were in fact romance fraudsters. What we did not know was whether two or more email addresses were controlled by the same real individual. Yet for the sake of not writing in a pedantic and awkward language, we referred 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. Our temporal focus was on the recent acts of fraud because we assumed that offenders, compared to those reported in prior years, were more likely to be *active* romance fraudsters (i.e., less likely to have desisted). The scrapping led us to obtain 546 unique email addresses. Our IRB had prohibited us from gathering demographic information on the sample, since it was not ideal to focus on information with unknown validity (i.e., the reported demographic traits may not match the offenders' actual traits).

To prevent issues concerning 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, using a program developed in Python. All emails were sent from the same generic Gmail address. However, not all fraudsters received the automated message because some email addresses were no longer active. 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 active email addresses, 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 was *Deterrence*, which was coded as a dichotomous variable. Those who received the deterrence message (i.e., individuals assigned to deterrent group) received a score of 1; otherwise, received a score of 0. We created three unique dependent variables to assess our hypotheses. The first variable, *Respond*, was coded as 1 if the fraudster responded to our message, and 0 if not. The second variable, *Words*, was 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*, was coded as 1 if the person's words were meant to generate a reply but did not deny wrongdoing; otherwise, coded as 0.

The data was analyzed in a stepwise fashion. First, descriptive statistics were calculated, followed by testing the first hypothesis. A chi-square test of independence was employed, followed by a robustness test to validate our findings. Next, in order to test the second hypothesis, we employed an independent sample t-test. An ANOVA test was also employed followed by a tukey kramer pairwise comparison test to determine which pair of means differed. In order to test the third hypothesis, a chi-square test of independence was again employed, followed by an additional robustness test to validate the findings. We were able to employ these simple models without controls due to the randomized nature of our field experiment. Throughout the process, it ensured 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.

Table 1: Descriptive Statistics for our Variables of Interest (N = 405).

	Observations	**Mean**	**Standard Deviation**	**Min**	**Max**
Respond	405	0.16	0.37	0	1
Words	405	7.88	46.2	0	529
Seeking Reply	65	0.78	0.41	0	1

To examine group differences in response probability, we conducted a chi-square test of independence. Recall that our first hypothesis was that romance fraudsters who received a deterrence message, instead of non-deterrence messages, will respond at a lower rate. Our findings supported this hypothesis. There was a significant difference in the response rate between those who received a deterrent message and those 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 those who received other messages was 20%. Results are presented in Table 2.

Table 2: Chi-Square Output on the Probability of Romance Fraudsters' Responses Between Deterrent and Non-Deterrent Groups (N= 405).

Groups	Not Responded (0)	Responded (1)	Total
Non-Deterrent	214	52	266
Deterrent	126	13	139
Total	340	65	405
	$x^2 = 7.04$		***p* = 0.008**

From the analysis presented in Table 2, it is unclear whether the two non-deterrent messages skewed the results. Therefore, we separately examined each of the three groups using a chi-square test of independence. Results indicated 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 "Hey" replied at a rate of 17%; those who were sent the promising message replied at a rate of 22%. Again, this finding supported our first hypothesis. Table 3 exhibits these results.

Table 3: Chi-Square Robustness Check on the Probability of Romance Fraudsters' Responses Between Three Groups (N= 405).

Groups	Not Responded (0)	Responded (1)	Total
Deterrent	126	13	139
Promising	100	28	128
Ambiguous	114	24	138
Total	340	65	405
	$x^2 = 8.03$		***p* = 0.0**

The second hypothesis of the study stated that among individuals who responded to our deterrence message, instead of non-deterrence messages, will use fewer words in the immediate responses. This hypothesis was tested using a one-tailed 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 statistically significant (t = 1.91, *p* = 0.03), thus supporting the second hypothesis as well.

Table 4: One-Tailed Independent Sample T-Test on the Number of Words in Romance Fraudsters' Immediate Responses (N = 405).

	Observations	Mean	Standard Error	Standard Deviation
Non-Deterrent	266	11	3.5	56.4
Deterrent	139	1.8	0.7	8.7
Combined	405	7.9	2.3	46.2
Diff		9.2	4.8	
t= 1.**86**			t = 1.91	***p* = 0.03**

Here too, however, it was possible that findings could be skewed by differences in the groups who received the non-deterrent messages. Therefore, we examined mean differences among the three groups using an ANOVA test. The results were marginally non-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 individuals who sent the promising message, and 7.6 words among those sent the ambiguous message.

Table 5: ANOVA Test on the Number of Words in Romance Fraudsters' Immediate Responses by Groups (N=405).

Groups	**Summary of Number of Words**		
	Mean	Standard Deviation	Frequency
Deterrent	1.83	8.69	139
Promising	14.80	70.83	128
Ambiguous	7.56	38.50	138
Total	7.88	46.19	405

Source	SS	DF	MS	F	Sig
Between Groups	11232	2	5616	2.65	0.07
Within Groups	850739	402	2116		
Total	861972	404	2134		

Using an ANOVA test alone, it was impossible to determine which pair of means differed. Therefore, we turned to the tukey pairwise comparison test. Table 6 presents that there is no 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). Though a marginally non-significant difference was observed in the mean number of words used between the deterrent and promising group (*p* = 0.06).

Table 6: Tukey Pairwise Comparison Test on the Number of Words in Romance Fraudsters' Immediate Responses by Groups (N=405).

			Tukey		**Tukey**
Messages Sent by Groups	Contrast	Standard Error	t	P > | t |	95% Confidence Interval
Deterrent vs Ambiguous	-5.72	5.53	-1.04	0.56	[-18.73, 7.28]
Promising vs Ambiguous	7.25	5.65	1.28	0.41	[-6.03, 20.52]
Promising vs Deterrent	12.97	5.64	2.30	0.06	[-.29, 26.23]

Exploratory Analysis

To better understand our data and, by extension, romance fraudsters, we conducted an exploratory analysis of the 65 responses that we had received to our messages. First, we qualitatively coded each person's textual message. These data were not large (~3,500 words), so we analyzed this content within a Microsoft Word document, rather than using a qualitative software package (e.g., NVivo). The qualitative data was organized into relatively unambiguous themes, or categories, reflective of our research foci. The most important emergent themes were *unambiguous denial* and a *desire to continue interaction.* The first of those was less prominent and, across the 65 responses, it was evident in only 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, ambiguous responses, was, in some respects, not a theme at all. 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 received the "Hey" 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.

Finally, we used our qualitative findings to construct a final hypothesis suitable for testing: Romance fraudsters who receive and respond to a deterrence message, instead of non-deterrence messages, have a lower probability of seeking *a reply without denying wrongdoing*. In order to test this hypothesis, we conducted a chi-square test of independence. Results, as presented in Table 7, demonstrate that fraudsters who received a deterrent message were 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 the support for this hypothesis as well.

Table 7: Chi-Square Output on the Probability of Romance Fraudsters' Seeking Reply Without Denying Wrongdoing Between Deterrent and Non-Deterrent Groups (N= 65).

Groups	**Not Seeking Reply or Denying Wrongdoing (0)**	**Seeking Reply Without Denying Wrongdoing (1)**	**Total**
Non-Deterrent	6	46	52
Deterrent	8	5	13
Total	14	51	65
	$x^2 = 15.39$		***p* = 0.000**

From the analysis presented in Table 7, it is unclear whether the two non-deterrent messages skewed the results. Therefore, we again separately examined each of the three groups using a chi-square test of independence. Results indicated there were 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%. This finding too supported our third hypothesis.

Table 8: Chi-Square Robustness Check on the Probability of Romance Fraudsters' Seeking Reply Without Denying Wrongdoing Between Three Groups (N= 65).

	Not Seeking Reply or Denying Wrongdoing (0)	**Seeking Reply Without Denying Wrongdoing (1)**	**Total**
Deterrent	8	5	13
Promising	1	27	28
Ambiguous	5	19	24
Total	14	51	65
	x^2 = 17.66		p **= 0.000**

Discussion

Cybercrime will continue to increase as society becomes more reliant on computers and networked devices (Shadmanfaat et al., 2020), so too will romance fraud. Research has examined its impact on victims and detailed its methods of execution. An interested reader is referred to the works of Whitty and her colleagues (Sorell & Whitty, 2019; Whitty, 2015, 2018; Whitty & Buchanan, 2012). Less scholarship focuses on whether, and how, to mitigate romance fraud. To build an evidence-base in this area, this study tested three hypotheses: Romance fraudsters who receive a deterrence message, instead of non-deterrence messages, respond at a lower rate(H1); Among those who respond, they use fewer words in their immediate responses(H2); such individuals less often seek a reply without denying wrongdoing (H3).

Our results show that romance fraudsters can be restrictively deterred (J. P. Gibbs, 1975; Jacobs, 1996b). In other words, and corroborating the findings of Maimon, Howell, and Burruss (2021), threatening romance fraudsters 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 deterrence 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 fraudsters 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-base for deterring and otherwise nudging offenders, analog and cyber, to commit fewer and lesser serious offenses (Maimon, Howell, & Burruss, 2021). 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 sends 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 methods 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, some of these email addresses may no longer be used by the romance fraudsters. However, this would deflate, rather than inflate, our findings. Fifth, 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. Finally, since we were only able to observe differences in responses, it is unclear if the "deterred" fraudsters continue to defraud their victims on other platforms using other tactics. If fraudsters continue to engage in romance fraud attempts, yet changed platforms or tactics, this too is evidence of (particularistic) restrictive deterrence.

Conclusion

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 (J. P. Gibbs, 1975), while providing a potential avenue for proactive mitigation strategies. We also provided additional evidence supporting the assumption of rationality and decision-making among cyber-offenders. The research exposed how fraudsters created fake profiles to lure their victims and established romantic relationships in order to extort money. A warning alarm is that such online romantic bliss can be very harmful. As time progresses, technological advancements continually change the cyber landscape. Human behavior, however, remains constant. Therefore, to ensure a safer cyberspace, more research is required into the human-factor in cybercrime (C. Jordan Howell & Burruss, 2020).

References

Bassey, S. A. (2020). Technology, environmental sustainability and the ethics of anthropoholism. *socialspacejournal.eu, 20*(2), 85-110. http://socialspacejournal.eu/Social%20Space%20Journal%2022020(20).pdf#page=85

Beccaria, C. (1995). *Beccaria: 'On Crimes and Punishments' and Other Writings* (R. Davies, Trans. R. Bellamy Ed.). Cambridge University Press. https://doi.org/10.1017/CBO9780511802485

Becker, G. S. (2000). Crime and Punishment: an Economic Approach. In N. G. Fielding, A. Clarke, & R. Witt (Eds.), *The Economic Dimensions of Crime* (pp. 13-68). Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-62853-7_2

Bentham, J. (1789). *An introduction to the principles of morals and legislation. Printed in the year 1780, and now first published. By Jeremy Bentham, of Lincoln's Inn, Esquire.* T. Payne, and Son, at the Mews Gate. https://www.earlymoderntexts.com/assets/pdfs/bentham1780.pdf

Blais, E., & Bacher, J.-L. (2007). Situational deterrence and claim padding: results from a randomized field experiment. *Journal of experimental criminology, 3*(4), 337-352. https://doi.org/10.1007/s11292-007-9043-z

Bossler, A. M. (2017). Need for debate on the implications of honeypot data for restrictive deterrence policies in cyberspace. *Criminology & Pub. Pol'y, 16*(3), 681-688. https://doi.org/10.1111/1745-9133.12322

Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice, 42*(5), 495-499. https://doi.org/10.1080/0735648X.2019.1692426

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law, 20*(3), 261-283. https://doi.org/10.1080/1068316X.2013.772180

Burruss, G., Howell, C. J., Bossler, A., & Holt, T. J. (2019). Self-perceptions of English and Welsh constables and sergeants preparedness for online crime: A latent class analysis. *Policing: An International Journal of Police Strategies and Management, 43*(1), 105-119. https://doi.org/10.1108/PIJPSM-08-2019-0142

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. https://doi.org/10.1093/bjc/azi059

Cornish, D. B., & Clarke, R. V. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending.* Transaction Publishers. https://books.google.com/books?id=VfmmAgAAQBAJ

Cross, C. (2020). Romance fraud. In T. Holt & A. Bossler (Eds.), *Palgrave handbook of international cybercrime and cyberdeviance.* London, UK: Palgrave.

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *The British Journal of Criminology, 58*(6), 1303-1322. https://doi.org/10.1093/bjc/azy005

Cross, C., & Holt, T. J. (2021). The use of military profiles in romance fraud schemes. *Victims & Offenders, 16*(3), 385-406. https://doi.org/10.1080/15564886.2020.1850582

Decker, J. F. (1972). Curbside Deterrence? An analysis of the effect of a slug-rejector device, coin-view window, and warning labels on slug usage in New York City parking meters. *Criminology, 10*(2), 127-142. https://doi.org/10.1111/j.1745-9125.1972.tb00549.x

Dickinson, T., & Wright, R. (2015). Gossip, decision-making and deterrence in drug markets. *British Journal of Criminology, 55*(6), 1263-1281. https://doi.org/10.1093/bjc/azv010

Dieko, S. N. (2020). La Convention de Mantego Bay à l'épreuve du différend frontalier entre Gabon et Guinée Équatoriale. *Res Militaris, 10*(2), 1-20. https://resmilitaris.net/index.php/2020/06/01/id1032023/

Federal Trade Commission. (2019). Romance scams rank number one on total reported losses. https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-losses

Geerken, M. R., & Gove, W. R. (1974). Deterrence: Some theoretical considerations. *Law & Society Review, 9*(3), 497-513. https://doi.org/10.2307/3053169

Gibbs, J. P. (1968). Crime, punishment, and deterrence. *The Southwestern Social Science Quarterly, 48*(4), 515-530. https://www.jstor.org/stable/42867909

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

Grabosky, P. (1996). Unintended Consequences of Crime Prevention. *Crime Prevention Studies, 5*(1), 25-56.

Green, G. S. (1985). General deterrence and television cable crime: A field experiment in social control. *Criminology, 23*(4), 629-645. https://doi.org/10.1111/j.1745-9125.1985.tb00367.x

Hobbes, T. (1969). *Leviathan, 1651.* Menston: Scolar P.

Howell, C. J., & Burruss, G. W. (2020). Datasets for Analysis of Cybercrime. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 207-219). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_15

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), 63-77. https://doi.org/10.5281/zenodo.495772

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

Jacobs, B. A. (1993). Undercover deception clues: A case of restrictive deterrence. *Criminology, 31*(2), 281-299. https://doi.org/10.1111/j.1745-9125.1993.tb01131.x

Jacobs, B. A. (1996a). Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence. *Justice Quarterly, 13*(3), 359-381. https://doi.org/10.1080/07418829600093011

Jacobs, B. A. (1996b). Crack dealers and restrictive deterrence: Identifying narcs. *Criminology, 34*(3), 409-431. https://doi.org/10.1111/j.1745-9125.1996.tb01213.x

Jacobs, B. A., & Cherbonneau, M. (2014). Auto theft and restrictive deterrence. *Justice quarterly, 31*(2), 344-367. https://doi.org/10.1080/07418825.2012.660977

Jacobs, B. A., & Miller, J. (1998). Crack dealing, gender, and arrest avoidance. *Social Problems, 45*(4), 550-569. https://doi.org/10.2307/3097212

Jacques, S., & Wright, R. (2008). The relevance of peace to studies of drug market violence. *Criminology, 46*(1), 221-254. https://doi.org/10.1111/j.1745-9125.2008.00102.x

Kashif, A., & Akhtar, Z. (2020). Detecting Deception using Reality Monitoring: A Multi-method Exploration. *International Journal of Criminal Justice Sciences, 15*(2), 191-215. http://dx.doi.org/10.5281/zenodo.3835429

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. https://doi.org/10.1002/mar.1029

Loewenstein, G. (1996). Out of control: Visceral influences on behavior. *Organizational behavior and human decision processes, 65*(3), 272-292. https://doi.org/10.1006/obhd.1996.0028

Lowman, J. (1992). Street prostitution control: Some Canadian reflections on the Finsbury Park experience. *The British Journal of Criminology, 32*(1), 1-17. https://doi.org/10.1093/oxfordjournals.bjc.a048162

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. https://doi.org/10.1111/1745-9125.12028

Maimon, D., Howell, C. J., & Burruss, G. W. (2021). Restrictive deterrence and the scope of hackers' reoffending: Findings from two randomized field trials. *Computers in Human Behavior, 125*, 106943. https://doi.org/10.1016/j.chb.2021.106943

Maimon, D., Howell, C. J., Moloney, M., & Park, Y. S. (2020). An examination of email fraudsters' modus operandi. *Crime & Delinquency*. https://doi.org/10.1177%2F0011128720968504

Maimon, D., Howell, C. J., Perkins, R. C., Muniz, C. N., & Berenblum, T. (2021). A Routine Activities Approach to Evidence-Based Risk Assessment: Findings From Two Simulated Phishing Attacks. *Social Science Computer Review*. https://doi.org/10.1177%2F08944393211046339

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. https://doi.org/10.2307/800696

Perkins, R. C., & Howell, C. J. (2021). Honeypots for Cybercrime Research. In *Researching Cybercrimes* (pp. 233-261). Springer. https://doi.org/10.1007/978-3-030-74837-1_12

Rämä, P., & Kulmala, R. (2000). Effects of variable message signs for slippery road conditions on driving speed and headways. *Transportation research part F: traffic psychology and behaviour*, *3*(2), 85-94. https://doi.org/10.1016/S1369-8478(00)00018-8

Rusch, J. J. (1999). The "Social Engineering" of Internet Fraud. *Internet Society Annual Conference* (pp. 1-11). http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm

Shadmanfaat, S. M., Howell, C. J., Muniz, C. N., Cochran, J. K., Kabiri, S., & Fontaine, E. M. (2020). Cyberbullying perpetration: An empirical test of social learning theory in Iran. *Deviant Behavior*, *41*(3), 278-293. https://doi.org/10.1080/01639625.2019.1565513

Smith, T., & Stamatakis, N. (2020). Defining Cybercrime in Terms of Routine Activity and Spatial Distribution: Issues and Concerns. *International Journal of Cyber Criminology, 14*(2), 433-459. http://dx.doi.org/10.5281/zenodo.4769989

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. https://doi.org/10.1080/00909889209365318

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). Springer. https://doi.org/10.1057/9781137457653_9

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. *Security Journal, 32*(3), 342-361. https://doi.org/10.1057/s41284-019-00166-w

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. https://doi.org/10.1109/TIFS.2019.2930479

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. https://doi.org/10.1111/1745-9133.12312

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal, 28*(4), 443-455. https://doi.org/10.1057/sj.2012.57

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behavior, and social networking, 21*(2), 105-109. https://doi.org/10.1089/cyber.2016.0729

Whitty, M. T. (2019). Who can spot an online romance scam? *Journal of Financial Crime, 26*(2), 623-633. https://doi.org/10.1108/JFC-06-2018-0053

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking, 15*(3), 181-183. https://doi.org/10.1089/cyber.2011.0352

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. https://doi.org/10.1177/1748895815603773

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. http://dx.doi.org/10.1177/0022427815587761