INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

Risk perception in digital contexts: questionnaire and pilot study

Laura Vozmediano, César San-Juan, Ana I. Vergara & Anita Lenneis*

Basque Country Institute. Universidad del País Vasco.
University of Vienna.*

Abstract

Fear of crime and risk perceptions related to crime are major topics of research in disciplines such as Criminology, but mainly in relation to the risk that street crime poses. Nowadays virtual settings are as familiar as the real ones for an increasing number of citizens worldwide. Cybercrime has become an objective risk and a source of worry, but fear and risk assessment have not been extensively studied yet. In this report, we present the results of a research developed in the University of the Basque Country for developing a questionnaire for measuring risk perception in digital contexts. We also offer the results of the pilot study for testing the psychometric properties of the questionnaire and discuss these first findings as well as future lines of research in this area.

Keywords: Cybercrime, risk perception, exposure, self-protective behaviours.

Introduction

Fear of crime and risk perceptions related to crime are major topics of research in several disciplines, including Environmental Psychology and Criminology (Hale, 1996). The work by Fisher & Nasar (1992) linking environmental attributes to the fear of crime and its subsequent development is a good example of the contributions made by environmental psychologists to the study of fear of crime in urban settings.

Nowadays virtual settings are as familiar as the real ones for an increasing number of citizens worldwide. Cybercrime has become an objective risk and a source of worry, but fear and risk assessment have not been extensively studied yet. Alshalan (2009) reported that 80% of surveyed internet users in the USA were "very worried" and found a higher fear among those previously victimized, those considering cybercrime as serious and among women. San Juan, Vozmediano & Vergara (2009) compared fear of cybercrime and street crime among residents in a safe Spanish city: they were more concerned with street crime, but the risk of being a victim of a cybercrime could be higher in this context.

Usage of the Internet is versatile (online banking, e-commerce, chatting…) and so are sources of risk and self-protection alternatives. This work presents a questionnaire developed to measure perceived risk of victimization in the Internet and exploring its relation to several relevant variables such as self-protective measures and typology of online behaviours. The report also offers the results of a pilot study for assessing reliability of proposed scales and exploring a model of online risk perception. This is the first step toward a research line aimed to investigate risk assessments in digital contexts.

INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

Cybercrime

Crime is a complex phenomenon. According to Brantingham & Brantinham (1991) a crime occurs when all of these four elements are present: a law, an offender, a target/ victim, and the place where the previous three coincide. There is no crime without laws defining the concrete behaviour as an offence. If there is no offender, there is no crime. Without a suitable target or victim, there is no crime. Without a space where these three spatio-temporal elements meet, there is no crime.

However, this proposal needs to be revised. Physical space seemed to be necessary to describe a committed crime. Nowadays, the presence of this fourth element is debatable. Cybercrime, crime committed through the internet, illustrates an actual threat for more and more citizens: the number of potential victims is growing since the number of people surfing the internet is steadily increasing. Thus, institutions like the Internet Complaint Center, which receives complaints about cybercrime in the United States, have been established (see Figure 1).

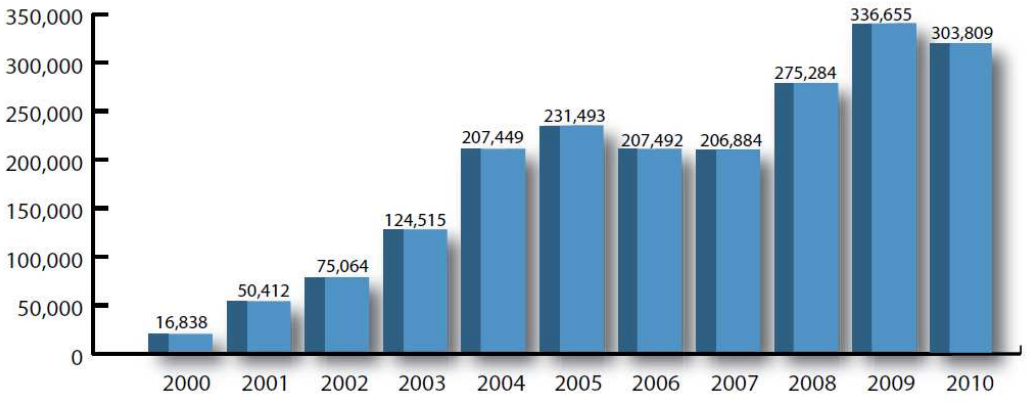

Figure 1. Development of the number of cybercrime complaints reported to the Internet Crime Complaint Center (USA).

Due to the properties of cybercrime, similarities and parallels between other types of crimes can be found. Nevertheless, the following distinctive features of cybercrime make it an especially interesting topic to explore from a criminological point of view:

- They can be committed easily
- They require little resources compared to the damage they cause
- They can be committed in a jurisdiction without physically being present in the geographical area to which such authority applies.

The offenders profit from legal loopholes in certain states. Some of them are known as cyber paradises, due to their lack of political intention to categorize or sanction these delinquent behaviours.

Nowadays it seems that the pursued objective of cyber-delinquents basically is short-term profit. It could be suggested that the *hacker* era –when illegal methods were used in order achieve prestige and publicity- has ended. Online-fraud experiences a constant grow, as well as the alert of specialized services of the security forces. Moreover, Trojan horses or Trojans, malicious software that can steal passwords, are becoming more worrying. They exceed the number of *phishing* attacks (sending massive amounts of deceptive e-mails in order to obtain usernames and passwords of several services) which are becoming less effective because of the rise of awareness during the past few years. However, despite this improvement in the available information, it has been found (San Juan et al., 2009) that at least in Spain, the actual awareness does not match the growing potential threats, as it be detailed below.

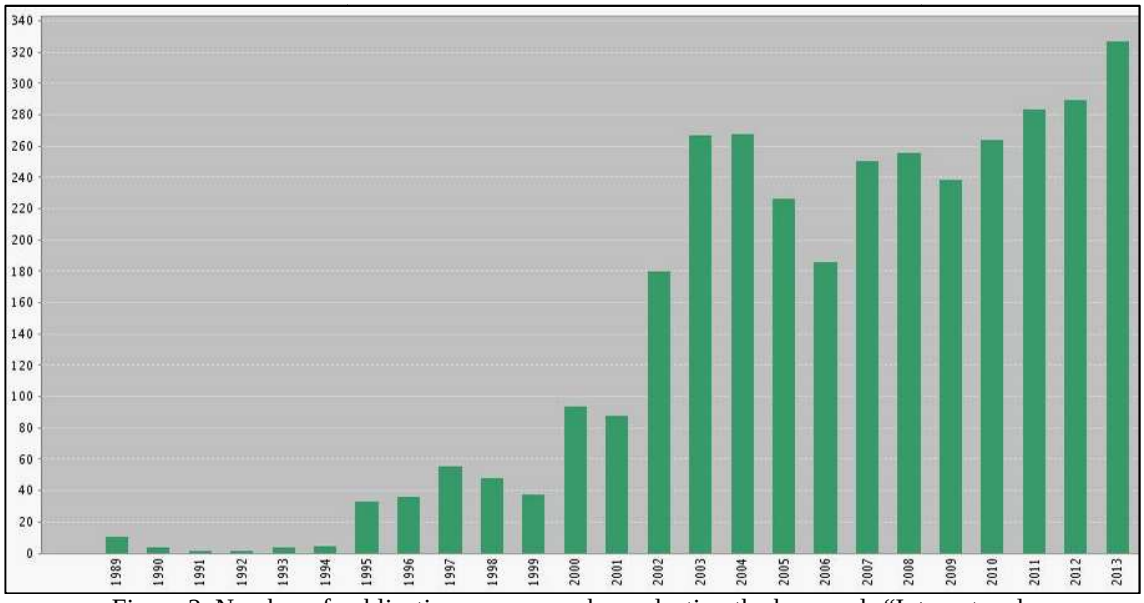

Figure 2. Number of publications per year when selecting the keywords "Internet and Crime" in the topic of the publication. Source: Web of Knowledge.

Due to the advancing increase in the number of internet surfers and, at the same time, the incidence of cybercrime, the interest of the scientific community in research related to crime in the internet and its victims has risen since 2003 and it has the highest number of publications in 2013 (see Figure 2). Therefore, when referring to scientific publications, there is a growing interest in this topic, although the interest in traditional crime still outweighs cybercrime -regarding the number of publications- in the Web of knowledge and other scientific sources.

Fear and risk related to Cybercrime

In the research of cybercrime many questions remain to be answered. The fear of cybercrime and risk perception related to this potential threat has received little attention

and therefore there are still few scientific publications specifically dealing with these topics.

However, the fear of suffering a crime in the Internet shows certain parallels to the fear of crime in urban spaces, which suggests that the research of cybercrime might equally be relevant. In both real and virtual scenarios the subject is provided with a big amount of stimuli and therefore it is necessary to select stimuli she or he needs to pay attention to. In both cases, the information about the risk of being a victim often is limited or biased. The perceptions of risk can be drawn away from reality. Thus, in the same sense that fear of crime in real life can inhibit certain behaviours, it is likely that the fear of suffering crime in the internet can also inhibit particular online behaviours such as buying goods, banking online, certain social activities, etc. On the other side, an exaggerated perception of security in comparison to objective risks could lead to risky patterns of internet surfing or usage.

Despite this, only few researchers have concentrated on the scientific research of fear of cybercrime. They have realized works about the assessment of risk of being a victim of crime while buying goods in the Internet, mainly published in scientific journals about new technologies. Similar works have been carried out by consulting firms or companies who directly work in online sales. These works aim to quantify the effects of perceptions of the users while realizing shopping in the internet.

Even with a reduced number of publications in scientific journals about this topic, some very interesting works can be cited, such as the article by Reisig, Pratt, and Holtfreter (2009). The authors used a sample of approximately 1000 Florida (USA) residents and found out that 57.6% of the respondents indicated that it was “somewhat likely” or “very likely” they would experience a damaging theft of their credit card

number while shopping in the internet. Furthermore, their results showed an association between a higher estimated risk and restricted internet use (shopping less, spending less time in the internet). On the other hand, the press published some surveys they were interested in regarding the trust of users and personal safety while using the internet. For instance a study which was carried out by the market research group TNS in 16 countries, who found that almost half of internet users developed distrust concerning the safety of their personal information while navigating the internet. However, we are unaware if it is possible that distrust leads to real fear of using the internet; and if distrust or fear influences certain behaviour.

Another interesting work is the monograph by Alshalan (2009). This author analyzed the data of the first survey carried out on a national level in the United States about victims of cybercrime. He found out that 80% of the respondents were "very worried" to turn into a victim of cybercrime. The fear of cybercrime was stronger among those who had suffered any sort of crime related to the internet before, those who believed that cybercrime was a serious problem, and among women- despite the fact that they are less affected of cybercrime; this goes along with classical results in the literature about crime in "real" contexts (Vozmediano, San Juan & Vergara, 2008).

In Spain, there are still few works about the fear of cybercrime. The findings of San Juan, Vozmediano, and Vergara (2009) point out that a significant percentage of subjects feared being victim of crime in a street, but had no fear in digital contexts -for example when providing sensitive information which includes online banking or online shopping- a behaviour that could imply a greater objective risk in a country and region that is quite safe in relation to street crime, when compared to other regions of Europe (San Juan, Vozmediano & Vergara, 2012). In this regard, the differences in fear of street

and virtual crime would be statistically incoherent, similar to fearing travelling in plane more than in car. The data are especially striking when taking into account the low rates of subjects who reported having obtained sufficient amount of information or resources to avoid being victim of cybercrime, according to the results of the same study (San Juan et al., 2009).

It must be taken into account, when studying subjective perceptions of crime, that fear of crime has been employed for describing a wide range of reactions to crime, often considering emotional but also cognitive and even behavioural aspects of the response to crime. We defend, following Ferraro (1995) and other relevant authors, that fear of crime is a useful concept for describing the fear, worries and anxieties related to the threat that crime poses. For analysing the cognitive assessment of this threat, the risk perception is a more useful concept. Both aspect of the subjective perception of crime – cybercrime, in this study-are relevant and interesting as an object of research. In this study, we have chosen the risk perception as the centre of interest, for initiating this line of research, while considering emotional aspects collecting information about worry of being a victim.

For measuring the risk perception related to cybercrime, we will follow the strategy that has been extensively used in the fear of crime literature (see Vozmediano et al., 2008 for a review of measures) and employ a scale that considers the estimated probability of becoming a victim. Therefore, we will be able to compare the cognitive assessment of the risk of cybercrime, in relation with other relevant variables such as Internet usage or knowledge.

Given that little is still known about fear of cybercrime and risk perceptions related to it -despite a few interesting publications- and taken into consideration that the

relation between fears and actual risks could be paradoxical, according to the results in San Juan et al. (2009), the purpose of this study was to initiate a research line in perceptions of cybercrime and their impact on online behaviours.

In this first study, we aimed to design and propose a questionnaire for reliably measuring perceptions of cybercrime and some related variables, to carry out a pilot study for determining the psychometric properties of the scale and to analyse the results of this pilot in order to propose a subsequent research agenda about subjective perceptions of cybercrime.

Method

Procedure and sample

The convenience sample for this pilot study was composed of 50 fist course college students of the degree in Criminology. They completed the questionnaire in their usual classroom, their participation was voluntary and they did not receive any compensation for it. No personal data that could identify the students was collected; therefore the information they provided was anonymous. The questionnaire that they fulfilled was used later in the course for discussing aspects related to cybercrime and its perception, but when they answered to the instrument they had no prior knowledge of these topics. Data was recorded and analysed using statistical software (SPSS).

The participants were mainly women (80%) and their ages varied from 18 to 40 years (M = 20.39, SD = 4.305). They used the Internet about four hours daily. All of the participants had their own computer, but 12% were using also public computers (for instance at the university or library) to gain access to the Internet. 92% used

smartphones too. 16% had game consoles that could also connect to the Internet, and 26% used some sort of tablet.

The main operating system of the participants' computers was Microsoft Windows (98%) and they reported that security was not very important (*M* = 2.15 in a five point scale, *SD* = 1.010) for choosing the operative system of their computers.

The majority of the students used Chrome as their primary Internet browser (72%), followed by Internet Explorer (18 %), Mozilla firefox (8%), and Safari (2%). They also reported that while choosing their internet browser, security played a small role (*M* = 2.35 in a five point scale, *SD* = 1.011). 94% of the respondents used an antivirus program.

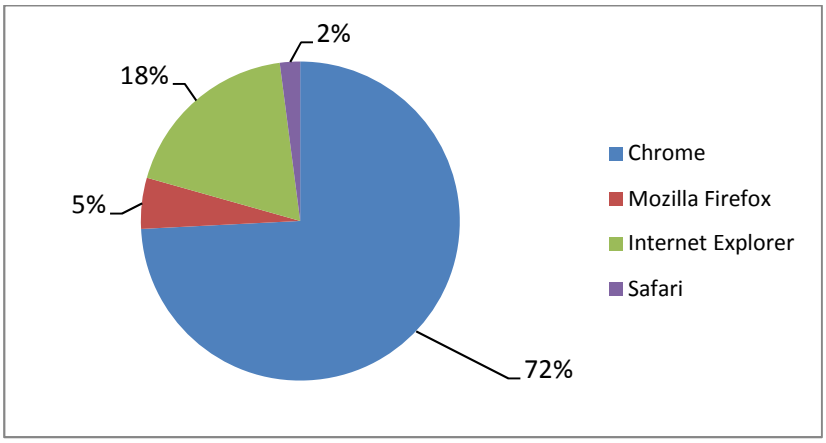

Figure 3. Internet browser used by the participants in the study.

In relation to social usage of the Internet, almost all participants (94%) were part of some social network. 80% had a facebook account, 84% used tuenti, 69.4% twitter and 2.1% linkedin.

Many of the participants already had been exposed to Internet crime or security problems. 72% had experienced a computer virus and 84% received spam or not desired e-mails, whereas only 6.3% has sufferd a spying attack, 14% the spread of data, photos, or private videos, 4% imitation or suppression of identity, 14% the access of the computer's content without permission, 24% the access of others to their accounts, and 2% credit card frauds. Among participants, 18% has been victims of cybermobbing and 6% of cybermobbing of sexual background, a worrying data in this young sample mainly composed of females.

Materials

The instrument designed by the research team aimed at measuring the risk perception in digital contexts and included questions about general socio-demographic information as well as scales for the main variables of interest in the study. These scales were:

- **Sociodemographic variables**. At the beginning of the questionnaire information about age, gender and city of residence was collected.
- **Risk exposure: Frequency of use**. This scale consisted of eighteen items that gathered information about the frequency of various uses of the internet, such us online shopping, sharing photos, and watching television online. Response options ranged from never to many times each day on a five-point- Likert-scale.
- **Sharing of personal data and information with third parties**. This scale consisted of ten items about different kinds of personal data and information being shared, such us mailing address, phone number, bank data, etc. Response options vary from never to always on a five-point- Likert scale.

- **Methods of self- protection**. This scale consisted of 15 items about precautions took when using the Internet. For instance, renewing software, logging one out, and actively looking for information regarding viruses or safe forms of using the internet. Response options range from never to always on a five-point-Likert scale.
- **Perceived ability.** This scale consisted of two items concerning one's perceived ability: having an excellent ability of computers and having enough knowledge to avoid being victim of cybercrime. Response options range from not agreeing at all to totally agreeing on a five-point-Likert scale, but also including the option to not know.
- **Vulnerability of the system**. This scale aims to measure with six items to what extent participants thought they were able to protect their computer from malware or possible attacks. Example items are the influence of the type of connection they used or whether the antivirus program would really protect them against viruses. Response options range from not agreeing at all to totally agreeing on a five-point-Likert scale, but also including the option to not know.
- **Concern of being a victim**. This scale consisted of 11 items asking about concerns of being a victim of cybercrime. Examples are viruses that harm the computer, receiving spam, credit card fraud, etc. Response options range from not concerned at all to very concerned on a five-point-Likert-scale.
- **Perception of risk: probability of becoming a victim**. This scale uses the same eleven items as concern of being a victim, but gathers information about the perceived probability of becoming a victim. Response options range from very unlikely to very likely on a five-point-Likert scale.

Results

The main objective of the pilot study was to obtain psychometric information about the reliability and one- dimensionality of the scales. As a result of the statistical analyses carried out, we could confirm that the scales proposed were composed by one dimension and had adequate levels of reliability. Only the scale *sharing of personal data and information with third parties* obtained a not optimum level of reliability, but it could be described as acceptable (α = .67). All the remaining scales that have been described in the methods section obtained very good values, from α = .80 to α = .91.

Having established that the psychometric properties of the scales were appropriate, a secondary objective was to offer information that could be useful for establishing a research agenda in the perceptions of online risk as well as fear of online risk. For achieving this goal, we performed descriptive and association analyses that would help us establishing some preliminary conclusions in this line of research.

Descriptive analyses gave us interesting information about online online behaviours and perceptions of college students. In relation to the risk exposure, measured by the frequency of various uses of the internet, participants used most of the services on a regular basis (*M* = 2.87, *SD* = 0.53). If we consider concrete uses, the participants most frequently used the internet on a daily basis to check and write e-mails (*M* = 4.5, *SD* = 0.61) or to hand in university work (*M* = 4.12, *SD* = 0.59).

Regarding to the practices of sharing personal data and information with third parties, participants did share personal information, but were aware of what they shared (*M* = 2.15, *SD* = 0.48). They most frequently shared pictures of themselves or close ones (*M* = 3.50, *SD* = 1.12) and their real name (*M* = 3.60, *SD* = 1.11) with others.

According to the results in methods of self-protection, our sample protected itself quite frequently against possible attacks (*M* = 3.0311, *SD* = 0.63405). The most popular methods were being sure that their passwords were not easily traceable (*M* = 4.35, *SD* = 1.110) and that they had good security settings in their social networks (*M* = 4.14, *SD* = 1.178).

In relation to perceived abilities to face the risks posed by cybercrime, participants perceived their general ability with computers as rather high (*M* = 3.42, *SD* = 3.30) and had medium knowledge to avoid being victim of cybercrime (*M* = 3.30, *SD* = 1.11).

Regarding to the judgement about the efficacy of services and strategies for protecting their computer from malware or possible attacks, participant overall trusted these services and strategies (*M* = 3.53, *SD* = 0.66), having the best consideration of their antivirus software (*M* = 3.92, *SD* = 0.77) and their filtering or blocking system (*M* = 3.93, *SD* = 0.77).

Finally, in regards to the concern of being a victim and the perception of risk, a certain level of discrepancy between these two variables was found. Overall the participants' worry about cybercrime was high (*M* = 3.73, *SD* = 0.88) compared to the perceived risk (*M* = 2.5, *SD* = 0.64). The security threats considered for answering to the concern and risk perception items were: (1) Virus that harms computer; (2) Spying of activities in the internet,; (3) Distribution of private data, photos, or videos; (4) Faking or displacing identity; (5) Access without permission to the computer's content; (6) Access of other people to one's accounts; (7) Bank movements without permission; (8) Non authorized use of one's credit cards; (9) Receiving spam or not desired e-mails;

INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

(10) Cyberbullying and (11) Cyberbullying of a sexual type. Figure 4 shows means for each security threats, contrasting the scores on worry and perceived risk.

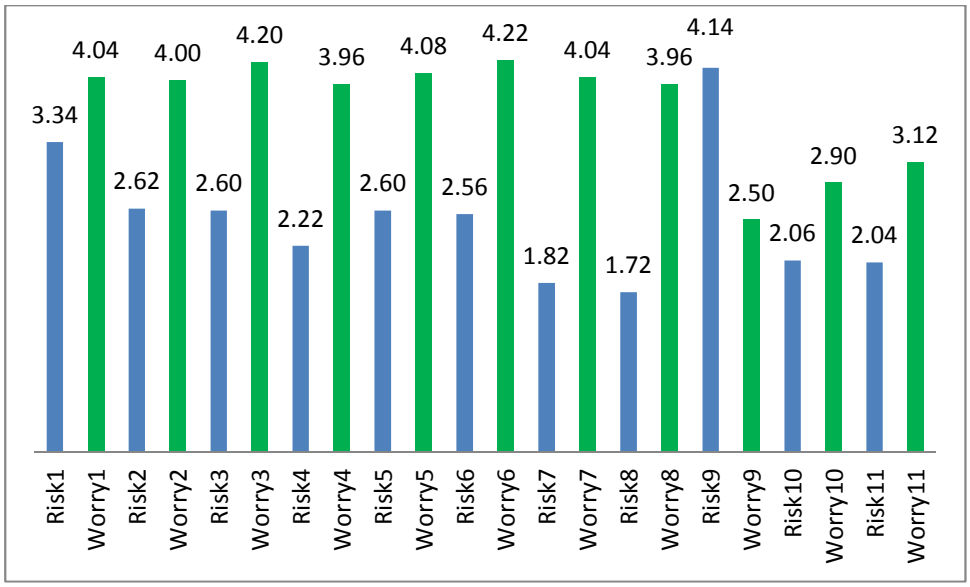

Figure 4. Contrast of the scores in every item of the scales *concern of being a victim* and *perception of risk*

Only for one security threat (spam emails) the concern was lower than the perceived risk. Participants estimated the probability of receiving spam e-mails as high (M = 4.14, SD = 0.86), but did not worry about it much (M = 2.50, SD = 1.035).

We also carried out correlation analyses, as a first attempt for understanding the relations among the variables included in the study. The main interest in this research was to begin understanding risk perception of cybercrime, measured as the estimated probability of becoming a victim of the described security threats. Therefore, we aimed to determine if exposure to risk was related to the variables included in the study. The only variable that showed a significant correlation to risk perception was worry about

the online security threats (r = 0.4, p = 0.00), but this was not the case for the rest of the scales included in the study.

Discussion

The objective of this project was to develop and test a questionnaire for measuring online risk perception, test its psychometric properties and establish futures lines of research in this field. According to the results of the pilot study, the reliability of the proposed scales is appropriate and therefore the development instrument can be used of assessing several variables related to risk perception and internet usage in Spanish.

The pilot study also offered a preliminary profile of how college students use Internet and perceive risks in our context. They were all using Internet on a daily basis and almost all participants were part of a social network, which means that they all are potential victims of cybercrime. Three quarter of the sample had experienced an internet virus -but less often other kinds of problems- showing that most of them had some experience being a victim of cybercrime. They perceived themselves as capable of protecting their computer and data, even when they shared frequently some types of personal information, mainly photographs. It is remarkable that worry about cybercrime was high among the participants, exceeding risk perception.

Worry was in fact the only variable related to risk perception, which was not associated with frequency of use, self-protection measures, what they thought about the vulnerability of the system and even with the previous victimization. These results were, to a certain extent, surprising, due to the lack of relation to behaviours and protective measures adopted. On the other hand, the results are coherent with a previous

study in our geographical context (the Basque Country, Spain) in which participants estimated the risk of cybercrime as lower that the risk posed by street crimes (San Juan et al., 2009). The overall perception of risk among participant was again moderate, even when the worry about those security threats was higher.

We must be cautious when interpreting the results of the study, due to some limitations, mainly related to sample, which was small and composed of college students. It will be necessary to carry out broader studies with bigger samples -both young samples with intensive use of the Internet, as the one in this study, and samples of general population- in order to verify if similar results arise. If this was the case, it would be advisable to include in future studies new variables that could contribute to propose a model of risk perception of cybercrime. If aspects related to exposure to risks, self-protective measures, perceived abilities and perceptions about vulnerability of the system are not related to risk perception, it could be a alternative to include more psychological variables in these future studies.

Studying the risk perception of concrete online threats separately could be another alternative for going forward in our understanding of these perceptions, since threats that imply damage to the computer and/or the data could answer to different dynamics than those implying a more serious danger for the affected individuals (such as cyber bullying). Therefore, we are still facing the challenge of understanding risk perceptions of cybercrime; more research initiatives will be needed for accessing to broader samples and develop a comprehensive model of risk perception of cybercrime.

References

Alshalan, A. (2009). *Cyber-Crime Fear and Victimization: An Analysis of a National Survey*. Saarbrücken: VDM Verlag Dr. Müller.

Brantingham, P. J. & Brantingham, P. L. (1991). *Environmental Criminology*. Prospect Heights, IL: Waveland Press.

Ferraro, K. F. (1995). Fear of crime. Interpreting Victimization Risk. Nueva York: State University of New York Press.

Fisher, B. & Nasar, J.L. (1992). Fear of crime in relation to three exterior site features: Prospect, refuge and escape. *Environment and Behavior, 24*, 35-65.

Hale, C. (1996). Fear of crime: A review of the literature. *International-Review-of-Victimology, 4*, 79-150.

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived Risk of Internet Theft Victimization Examining the Effects of Social Vulnerability and Financial Impulsivity. *Criminal Justice and Behavior, 36*, 369-384.

San Juan, C., Vozmediano, L. & Vergara, A.I. (2009). Miedo al delito en contextos digitales: Un estudio con población urbana. *Eguzkilore, Cuadernos del Instituto Vasco de Criminología*, *23*, 175-190.

Vozmediano, L., San Juan, C., & Vergara, A. I. (2008). Problemas de medición del miedo al delito: algunas respuestas teóricas y técnicas. *Revista electrónica de ciencia penal y criminología, 10-07.* Disponible en Internet: http://criminet.ugr.es/recpc/