Copyright © 2020 International Journal of Cyber Criminology – ISSN: 0974–2891
January – June 2020. Vol. 14(1): 139–155. DOI: 10.5281/zenodo.3744874
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Understanding Target Suitability in Cyberspace: An International Comparison of Cyber Victimization Processes

Fernando Miró-Llinares[1]
Miguel Hernandez University of Elche, Spain

Jacqueline Drew[2] & Michael Townsley[3]
Griffith University, Australia

Abstract

Economic forms of cybercrime affect millions of people around the world. Preparatory crimes such as spam, scam and malware are increasingly enacted by cybercriminals. However, literature has shown that some people are more vulnerable than others to these types of attacks and this may be a circumstance that varies cross-nationally. Using a comparative research design, behaviors that are associated with a higher probability of victimization by economic preparatory crimes are identified. The results obtained from two samples, one Spanish and one Australian, show that despite similar victimization prevalence, the correlates of routine activities vary substantially. While 6 of the 11 behaviors analyzed were similar, other substantial differences were found. The greatest risk for Spanish participants is online shopping, while for Australians it is downloading files. Differences were also found for use of antivirus, pirated software, contacting strangers and taking part in video conferences. Based on the current research, it is concluded that cyber victimization should focus on identifying nuances in the daily activities performed by online users, rather than on broader constructs such as interaction or visibility. Further, preventive strategies must take into account differences in routine behaviors across different geographical areas.

Keywords: Cybercrime; Cybercrime Victimization; Cybercrime Prevention; Routine Activities Approach.

Introduction

Cybercrime now represents the fastest growing crime type. Whilst statistics around cybercrime vary and issues of under-reporting leads to the underestimation of its prevalence, the occurrence of cybercrime is still startling (Caneppele & Aebi, 2017). These

[1] Professor of Criminology and Chair of the Crimina Research Centre for the Study and Prevention of Crime, Miguel Hernandez University of Elche. Email: f.miro@crimina.es
[2] Senior Lecturer, Griffith Criminology Institute, Griffith University, Messines Ridge Road, Mt Gravatt, Queensland, Australia. Email: j.drew@griffith.edu.au
[3] Associate Professor, Griffith Criminology Institute, Griffith University, Messines Ridge Road, Mt Gravatt, Queensland, Australia. Email: m.townsley@griffith.edu.au

types of crime have increased exponentially as online connectivity expands to all corners of the world (Holt & Bossler, 2014). The United Nations report that 84% of the world population now live in an area where mobile-broadband is available and 47% actively use the internet (United Nations, 2016). Recently, cybercrime was, for the first time, included in the Crime Survey for England and Wales. According to the UK Office for National Statistics, in 2017 it overtook traditional crimes, such as burglary and theft of vehicles, online crimes now represent the most commonly experienced offence types (Bangs, 2017). In 2018, the FBI through its Internet Crime Complaint Center (IC3) received 351,937 cybercrime complaints with reported losses totalling more than US$2.7 billion.

Many types of cybercrime threats are faced by Internet users. Email-based social engineering attacks are one of the most commonly reported types of cybercrime (Cross, Smith & Richards, 2014; IC3, 2018). Fraudulent emails, including spam and phishing emails, typically seek to gain personal or financial information from the victim in order to directly financially exploit the victim or are used as steps in identity theft and subsequent, fraud (Cross, 2015; Gupta, Arachchilage & Psannis, 2018). Infection by malware, delivered through fraudulent emails or websites, is conducted to infect the users' computers to gain access to personal and financial information (Bossler & Holt, 2009). It can involve the installation of software that allows the offender to monitor all actions undertaken by the victim on the infected system, such as is the case with key logging software, allowing the offender to harvest online passwords to, for example, bank accounts. A recent threat report produced by the Australian Cyber Security Centre (ACSC, 2017) indicated that offenders are becoming better at both targeting and launching more sophisticated attacks in their delivery of credential-harvesting malware.

We take the unique approach of conceptualizing specific types of cyber-attacks as primarily preparatory acts. Preparatory attacks are offender-initiated actions or behaviors that allow the offender to more easily target and exploit the target at some later time. Examples of preparatory attacks include 'victimization by scam,' 'victimization by spam,' and 'victimization by malware.' Scams, spam and malware are typically used to harvest and collect personal and/or financial information. At this stage, cybercrime has occurred but it is not until victims interact or respond to offenders and offenders use the harvested information to financial exploit or use stolen identity, that their ultimate goal of cyber fraud has been achieved.

This research seeks to address an important gap in the literature by focusing on the effectiveness of protective behaviors that may be enacted by potential victims when they are targeted by these specific types of preparatory attacks. More effective use of protective behaviors by victims who experience a preparatory cyber-attack is likely to reduce subsequent crimes, most notably financial exploitation and theft of other personal information. The research is important as it focuses on the first possible crime prevention intervention point for many types of financial exploitation crimes enacted in cyber space. By better understanding and addressing preparatory crimes, it may be possible to more effective interrupt and prevent specific cybercrimes that flow from these initial preparatory and harvesting methodologies.

As identified, the purpose of this study is to identify online behaviors of potential victims that make them at increased risk of preparatory acts of fraudulent emails (victimization by scam and victimization by spam) and malicious software (victimization by malware). To do so, we recruited representative samples from Spain and Australia to complete a survey assessing the extent of their online behavior and victimization history.

While fairly similar victimization prevalence rates were observed between the samples, differences between online behaviors and the attendant risk factors emerged. These results suggest targeted prevention advice for particular populations is likely to be most effective in curbing cybercrime.

1. Literature Review

1.1. Cybercrime dynamics

Holt and Bossler (2010) called for further research to examine whether risk factors, both individual and situational, predict all types of cybercrime victimization equally. More recently, it has been concluded that existing research often fails to differentiate and acknowledge that different cybercrimes may need to be studied as distinct types of crimes (Bergmann, Dreibigacker, vonSkarczinski & Wollinger, 2018).

Internet-enabled criminality, unlike offending in the real world, has virtually no transaction or distribution costs for targeting potential victims (Miró-Llinares, 2011). Targeting one person takes almost the same effort as targeting millions of Internet users. The offender can afford to be indiscriminate in targeting victims of preparatory crimes, such as malware and fraudulent emails, given the resources and effort required to target victims in these ways. The offender can then become more focused based on the success of preparatory crimes, narrowing their victimization pool to those individuals who 'fall' for the preparatory attack.

The almost unlimited nature of victim targeting through the cyber-attacks described has implications for our understanding of the commission process and, importantly, crime prevention. Existing scholarly knowledge about fraud and other economic crimes may not translate to economic cybercrime. Numerous studies provide detailed accounts of the lengths motivated burglars (Rengert & Wasilchick, 1985; Cromwell, Olson, & Avary, 1991), robbers (Miller, 1998) and fraudsters (Morley, Ball & Ormerod, 2006; Policastro & Payne, 2015) go to find suitable targets. But if there is next to no friction in locating suitable targets online, do offenders need to carefully choose targets for cyber-attacks, particularly preparatory attacks? Can they simply cast a wide net confident that if they are successful even a fraction of a percent of times, they will be more successful than the best terrestrial fraudster? What are the implications for potential victims? Unlike more established crimes, comparatively less is known about offender methodologies online and critically, what potential victims can do to protect themselves. It is of significant importance to understand how the process of victimization occurs within these types of preparatory cyber-attacks and in turn, how to prevent the final stage of the crime being facilitated, that is actual financial theft and exploitation. Routine activities approach (RAA) provides a framework that is applicable or at least, adaptable to understanding preparatory cyber-attacks.

1.2. Cybercrime victimization: A routine activities lens

At the micro level, routine activities approach (RAA) proposes that crime is possible when a motivated offender meets a suitable target in the absence of a capable guardian (Cohen & Felson, 1979). While originally developed for direct predatory crime, RAA has become the most widely used approach to analysis of economic victimization from a social science perspective.

There is a growing body of empirical work that has used RAA to guide our evolving understanding of cybercrime (e.g., Bossler & Holt, 2010). RAA has been applied to crimes including malware (Bossler & Holt, 2009), phishing (Leukfeldt, 2014), consumer fraud (Van Wilsem, 2013), stalking (Reyns, Henson & Fisher, 2011), sexual solicitation (Marcum, Rickets & Higgins, 2010), defamation (Ngo & Paternoster, 2011) and harassment (Miró-Llinares, 2015). Varying levels of success in the application of the theory has largely depended on the crime type studied (Leukfeldt & Yar, 2016). Empirical research has supported linkages between opportunity-based risk factors and victimization (McNeeley, 2015). Relevant to the current study, Choi (2008) examined victimization by computer viruses, through email and downloading. Risk of virus victimization was reduced by technical guardianship, which included use of anti-virus software. Engaging in risky online behaviours and online leisure activities increased virus victimization. Pratt, Holtfreter and Reisig (2010) studied 13 types of consumer fraud. The study examined contact by offenders through internet-related means, including auction sites, websites and email. Hours spent online and website purchasing both increased the likelihood of being targeted for internet fraud. Bossler and Holt's (2009) research focusing on malware victimization failed to find strong relationships between data loss from malware and online behaviors and guardianship. This is contrary to the findings of Leukfeldt and Yar (2016) who found malware victimization was explained by visibility and accessibility factors (i.e., frequency of internet use, targeted and untargeted browsing behavior, online gaming, downloading and buying online).

As concluded by Leukfeldt and Yar (2016) a review of empirical studies using the RAA does not yet provide a clear answer as to the applicability of this approach to the diverse range of cybercrimes. Whilst findings related to visibility factors is relatively consistent, that is online routine behaviors is associated with cybercrime victimization, the role of guardianship is less definitive (Holt & Bossler, 2016).

1.3. Targets, guardianship and victimization in cyber places

1.3.1. Target visibility and cyber victimization

Target suitability and target visibility has been conceptualized in the literature to involve use of information technologies and constructs relevant to the specific activities and time spent in cyberspace (Hutchings and Hayes, 2008; Pratt et al., 2010). Typically, studies of cybercrime victimization will include a measure of time spent online, relying on the premise that online presence will increase visibility (Drew & Farrell, 2018; Miró-Llinares, 2012). Reyns, Fisher, Bossler and Holt (2018) found that time spent in opportunity-producing routine activities increases victimization risk for harassment, identity theft and receiving nude/explicit emails. Researchers have also sought to understand how specific activities enacted online may influence target visibility and suitability (Drew & Farrell, 2018; Miró-Llinares, 2015). Mixed findings have been reported for the relationship between online opportunity and victimization (Holt & Bossler, 2016; Jansen & Leukfeldt, 2015; Reyns, 2017; Vakhitova, Reynald & Townsley, 2016).

Understanding how the actions and decisions of internet users' impact on victimization has been studied by some researchers using the notion of online or internet lifestyle factors, drawing from the tenets of lifestyle-exposure theory. In recent literature examining cybercrime victimization, both concepts of RAA and lifestyle-exposure theory have been utilized to explore target suitability (Bossler & Holt, 2009; McNeeley, 2015). Choi (2008) constructs the concept of an 'online lifestyle' using three scales. These include a 'vocational and leisure activities scale,' which evaluates instant messaging use, time spent downloading files, shopping, spending time on the Internet for entertainment, spending time on the Internet when bored, watching news, checking and sending emails. The scale labelled 'risky leisure activities,' includes visiting web sites, downloading free games, downloading free music, and downloading free movies. The final scale is the 'risky vocational activities', a scale that includes opening email attachments, clicking on web-links in e-mails, opening files or attachments received through instant messaging, and clicking on pop-up messages.

Similarly, Bossler and Holt (2009) proposed two categories of target suitability: the first consists of factors related to routine computer use, which includes computer ownership, Internet connection speed, and time spent per week shopping, playing video games, checking e-mail, using chat rooms, instant messaging, downloading files, programming, using on-line banking or social networks. The second consists of factors related to deviant user behavior on the Internet, such as using pirated software, looking at pornography, guessing someone else's password, accessing someone else's computer.

This research in part addresses the concept of target visibility, its role in crime outcomes and how a greater understanding of visibility can inform victimization and crime prevention. We argue that it is behavior of those targeted online that makes them more or less visible and, in turn, more or less accessible to the potential offender. The difference in this research is that we focus specifically on undertaking a detailed analysis of a subset of cybercrimes, cybercrimes we view as preparatory crimes that have little to no associated victim targeting.

1.3.2. Self-protection and capable guardianship in cyberspace

Drawing on previous research applying RAA to cybercrime we must also consider the concepts of self-protective behaviors and guardianship. Leukfeldt and Yar (2016) concluded that the role of guardianship is cybercrime victimization is less clear. We ague in this paper that the guardianship and self-protective behaviors may be more relevant and produce greater explanatory power when focusing on preparatory cyber-attacks. Offender actions such as fraudulent emails and malware are cyber-attacks that if prevented, through protective behaviors enacted by potential victims, reduce subsequent crimes involving financial and identity exploitation.

Previously, target suitability and visibility was discussed in respect to the relationship between time spent online and the types of activities and in turn, risk of cybercrime victimization. Protective behaviors enacted by potential victims that may also influence the success of cyber-attacks against them. Often in the online context, self-protection is conceptualised as the installation of virus software, firewalls and not providing information in response to unsolicited emails (e.g., Drew & Farrell, 2018).

Choi (2008) discusses the 'digital guardian' construct, which consists of two variables, one related to the use of security software (antivirus, antispyware and firewall programs), and another related to the duration of security software use. This is linked to victimization by malware infection. In order to determine risk factors associated with the loss of information from a malware infection, Bossler and Holt (2009) also consider whether or not the user has installed different kinds of security software on the computer system. The other factors related to the capable guardian construct that appear in the literature are associated with the victim's computer skills or knowledge of the presence of protective software on systems that might impede victimization (Miró-Llinares, 2012). Ngo and Paternoster (2011) study of social victimization by malware infection and phishing constructed capable guardianship as the union of physical guardianship (use of security software such as antivirus, anti-spyware, and firewall programs) and social guardianship (defined as computer skills and knowledge of Internet risks, acquired by attending classes or self-informing through Internet websites). Typically, the focus is on the relevance of the self-protective behavior of the victim themselves.

The current study is interested in exploring how the actions and behaviors of victims when online, if better understood through a cybercrime scaffolding framework including preparatory cyber-attacks, could be used to construct better self-protection and guardianship behaviors of potential victims. This research will examine how different types of online visibility is associated with increased likelihood of being a victim of a preparatory cyber-attack, specifically fraudulent emails (victimization by scam and victimization by spam) and malicious software (victimization by malware).

Understanding the relationship between visibility and preparatory cyber-attacks can be used to interrupt the cybercrime offending and victimization trajectory. Reducing the experience of cyber-attacks will in turn reduce the ability of offenders to undertake follow-on cybercrimes that financially exploit victims and/or compromise identity. In this way, focusing and impacting on preparatory cybercrimes addresses the first stage of victimization and could be interpreted as an early intervention approach that would reduce potential harm and prevent further victimization.

1.3.3. Routine activities in cyber places

The third essential element for the analysis of victimization in the framework of everyday activities is the crime place. In the same way that places play an essential role in the dynamics of victimization in physical space, cyber places are determinant for analyzing the type of convergence that takes place between offenders and victims and, therefore, the type of cybervictimization possible (Miró-Llinares & Johnson, 2018). Depending on how these virtual spaces are configured, offenders and victims may converge in one way or another (e.g., allowing streaming or store and forward modalities of contact). Based on the place they pass through, the objectives will be more or less visible, users will be able to exercise greater or lesser social control, and potential victims will have some resources or others to encourage their self-protection. In addition, the type of activity that users carry out in a given cyber place will shape the day-to-day activities carried out there and thus also their convergence.

Depending on how these elements are combined at each place, cybercrime will describe specific patterns. For example, Miró-Llinares, Moneva and Esteve (2018) studied the environmental characteristics of Twitter's cyber places at the micro level and found that some digital microenvironments are more likely to host hate speech than others. In order to identify specific cybervictimization patterns experienced by online users, different cyber places in which Internet users carry out their daily activities such as online shopping portals, instant messaging applications, social networks, forums and blogs, or download sites, among others, have been considered in this research.

2. Current Study

In conclusion, applying RAA to cybercrime leads to at least two conclusions. The first is that victims engage in behaviors that affect their own victimization when performing their routine activities in specific cyber places, even when they are not being specifically targeted by offenders. The second is that current understanding of target suitability, target visibility and the role of self-protective behaviors and guardianship in cyberspace is limited. More needs to be known about how victim behaviors contribute to and interact with offender methodologies, increasing target suitability and leading to increased risk of online victimization.

The objective of the current study is to identify risk factors that are associated with the preparatory steps or cyber-attacks enacted by offenders to financial de-fraud or exploit victims in cyberspace in two different samples (i.e. Spanish and Australian) using a comparative research design. Receiving spam emails, receiving phishing emails and infection by malware are conceptualized as some of the most commonly experienced types of approaches that are undertaken by offenders. Further they are the types of cyber-attacks which are most commonly experienced by potential victims within the routine activities of Internet users. It is argued that application of RAA to cybervictimization studies should focus on the target's suitability and visibility, those behaviors that make potential victims more visible and more accessible to cyber-attacks. Accordingly, this study examines the visibility of potential victims. Visibility is defined as the degree of interaction and exposure that the victim has to cyber-attacks. It is hypothesized that the risk of experiencing spam, scam, and malware victimization will increase as a function of the amount of engagement that a potential victim has with specific types of activities in cyberspace, for example online shopping, playing online games, using social networks and posting in forums and blogs.

3. Method

3.1. Sample

To select the subjects, we used a probabilistic sample stratified by sex, age, and place of residence. For the Spanish sample, the data was collected using a Computer Assisted Telephone Interviewing (CATI) system with an interview duration of up to 15 minutes. Additional criteria for participant inclusion were 1) using the Internet a minimum of 8 hours per week and 2) a minimum age of 18 and a maximum age of 65. For the Australian sample, the sample was accessed via a data collection service, Survey Sampling International (SSI; now known as dynata) (https://www.dynata.com/) from their database of survey respondents. The data collection agency was asked to provide a sample that was representative of the Australian population on the criteria of age (18 to 65 years) and gender.

The Spanish sample is made up of 500 Spanish adults, of whom 222 (44.4%) were men and 278 (55.6%) women, with a mean age of 40.21 (SD =12.57). A minimum age of 18 was set with the intention of avoiding the problems presented by obtaining data from minors. The upper age limit was set at 65, as the percentage of Internet users over the age of 65 is very low in Spain (Instituto Nacional de Estadística, 2011). The Australian sample is made up of 574 Australian adults, of whom 257 (44.8%) were men and 315 (54.9%) women. Two (2) participants identified as "Other". As per the Spanish survey, the minimum age of participants was 18 and the maximum age was 65. The modal age was between 25 and 34 years.

3.2. Instrument

For the study, a survey was originally prepared in Spanish. In order to ensure the validity of survey content, professionals from different areas (jurists, criminologists and methodologists) were consulted with the goal of developing a rigorous instrument. The survey was made up of four types of questions: one filter question, 'How many hours per week do you spend connected to the Internet?' to identify subjects who were connected to the Internet at least 8 hours per week; three socio-demographic questions (sex, age, place of residence (autonomous community)); questions about routine activities on the Internet; and questions related to preparatory economic cyber victimization: victimization by scam, victimization by spam, and victimization by malware. In order to verify that the instrument functioned reliably, a pilot study (N = 100) was conducted. The survey was conducted via a telephone.

The Spanish survey was translated to English by a professional translation service for use with the Australian sample. Small adjustments to wording were made to localize questions to the target sample. For the Australian sample, data was collected through an online survey tool.

3.3. Variables

3.3.1. Dependent variables

Three dependent variables were included in the study: 'victimization by scam,' 'victimization by spam,' and 'victimization by malware.' The 'victimization by scam' variable was obtained by asking: 'Have you ever received an email proposing some kind of favor or economic transaction that you suspected might have been fraudulent?' Respondents who answered in the affirmative were categorized as 'victim' and those who answered in the negative were categorized as 'non-victim.'

The 'victimization by spam' variable was created by asking: 'Have you ever received an email for which you suspected that the sender's identity was false?' Those who answered in the affirmative were included in the category of 'victim' and those who answered in the negative were categorized as 'non-victim.'

Finally, the 'victimization by malware' variable refers to users who have been warned by their antivirus software of the presence of a virus ('Has your antivirus software ever warned you of the presence of a virus?'). Subjects who answered in the affirmative were categorized as 'victim' and those who answered in the negative were categorized as 'non-victim.' The value of this variable depended on the user verifying they have been infected, while knowing that in many cases, especially in the absence of antivirus software, an attack may have occurred and an infection might exist without the user's knowledge. However, short of obtaining access to users' machines, we had no other feasible means of determining victimization by malware infection.

3.3.2. Independent variables

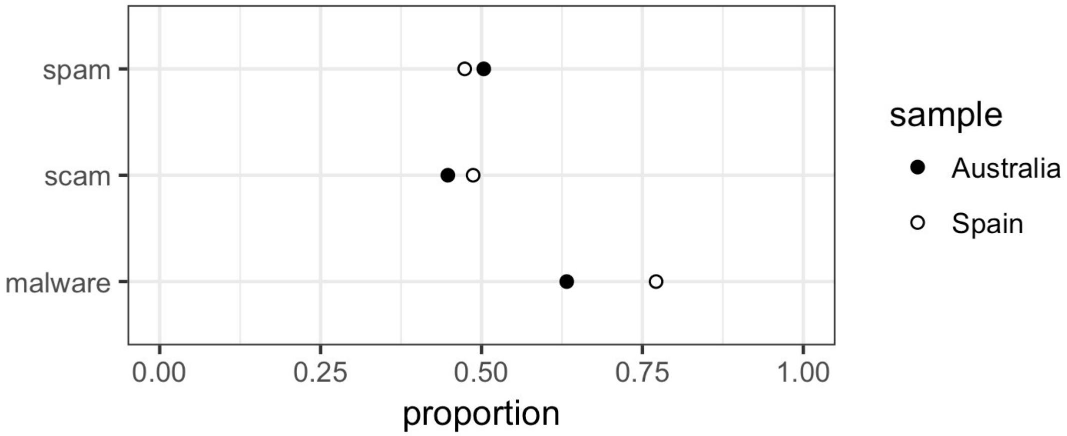
Eleven variables were included to measure users' routine activities on the Internet that make them 'suitable' targets by asking if they had ever: shopped online, used an instant messaging service, used social networks, posted in forums or blogs, played online video games, participated in teleconferences, consumed pornography, downloaded files, had contact with strangers, not used antivirus software, and used pirated software. All variables were recorded as dichotomous (Yes/No).

4. Results

4.1. Dependent variables

Figure 1 contains the victimization prevalence for each dependent variable for both samples.

Figure 1. Comparison of victimization type by country



Only malware was observed to have a difference between the samples but this is largely due to the number of respondents in the Australian sample who did not answer definitively (see Table 1). The only major difference in victimization prevalence between the two samples was for malware with the Spanish sample more likely to be victimized by this type of preparatory attack.

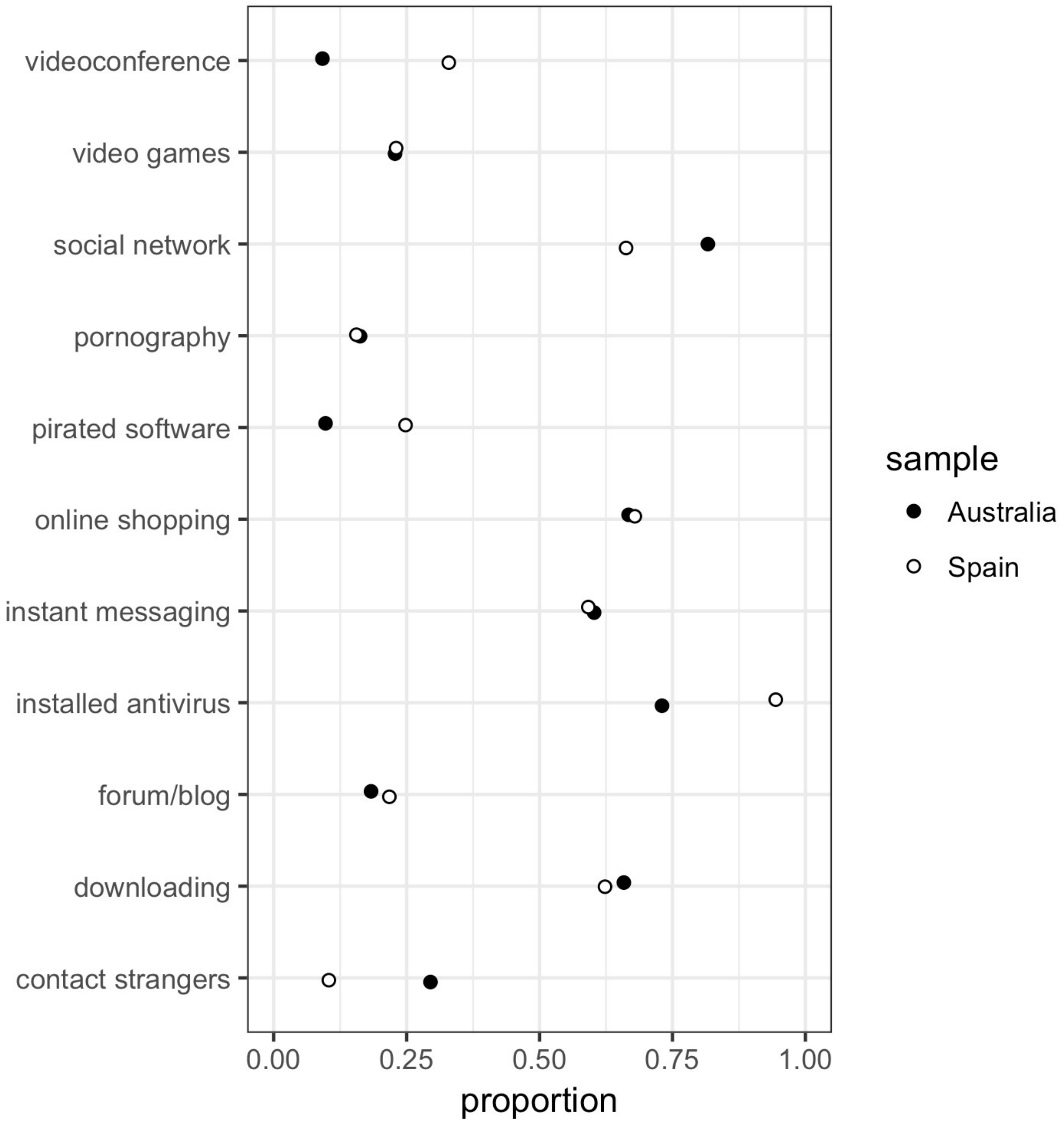
Table 1. Frequencies for Dependent Variables

	Malware (%)	Scam (%)	Spam (%)
Australian Sample			
NA	18 (3.1)	0 (0)	0 (0)
non-victim	193 (33.6)	317 (55.2)	285 (49.7)
victim	363 (63.2)	257 (44.8)	289 (50.3)
Spanish Sample			
non-victim	108 (22.9)	237 (51.3)	242 (52.6)
victim	364 (77.1)	225 (48.7)	218 (47.4)

4.2. Independent variables

Figure 2 contains the proportions of survey respondents for both samples who answered in the affirmative for each of the online behaviors. For most variables there was a high degree of correspondence between the samples. Major differences were observed for five out of 11 variables. Differences were found for contact strangers, installing antivirus, pirated software, using social networks and participating in videoconferences.

Figure 2. Comparison of online behaviors by country



4.3. Model results

Logistic models were computed for the three dependent variables and both samples (i.e. six models in total), see Tables 2 and 3. Overall, model performance was better for the Spanish sample (Nagelkerke R^2 = .25, .21 and .11) compared to the Australian sample (Nagelkerke R^2 = .10, .11 and .06).

Table 2. Logistic Regression of Scam, Spam and Malware - Australian Sample.

	Scam	Spam	Malware
contact strangers	0.481** (0.199)	0.650*** (0.202)	0.216 (0.207)
downloading	0.785*** (0.201)	0.679*** (0.197	0.631*** (0.194)
forum/blog	−0.221 (0.256)	0.085 (0.257)	0.001 (0.263)
instant messaging	−0.149 (0.205)	−0.120 (0.205)	−0.185 (0.209)
installed antivirus	0.343 (0.209)	0.554*** (0.209)	
online shopping	0.368* (0.193)	−0.061 (0.192)	0.136 (0.193)
pirated software	−0.290 (0.308)	0.027 (0.313)	−0.198 (0.325)
pornography	0.437* (0.259)	0.725*** (0.272)	0.645** (0.292)
social network	0.078 (0.257)	0.140 (0.255)	0.174 (0.256)
video games	0.020 (0.227)	−0.141 (0.230)	0.025 (0.238)
videoconference	−0.034 (0.326)	−0.006 (0.336)	0.545 (0.379)
Constant	−0.455 (0.401)	−1.404*** (0.422)	−1.826*** (0.455)
Nagelkerke R2	0.095	0.11	0.063
Observations	574	574	574
Log Likelihood	−373.554	−373.105	−362.108

Note: ⋆ = p<0.1; ⋆⋆ = p<0.05; ⋆⋆⋆ = p < .01
Coefficients are log odds.
Antivirus was not included for Malware model because the item used to determine this form of victimization includes the use of antivirus software.

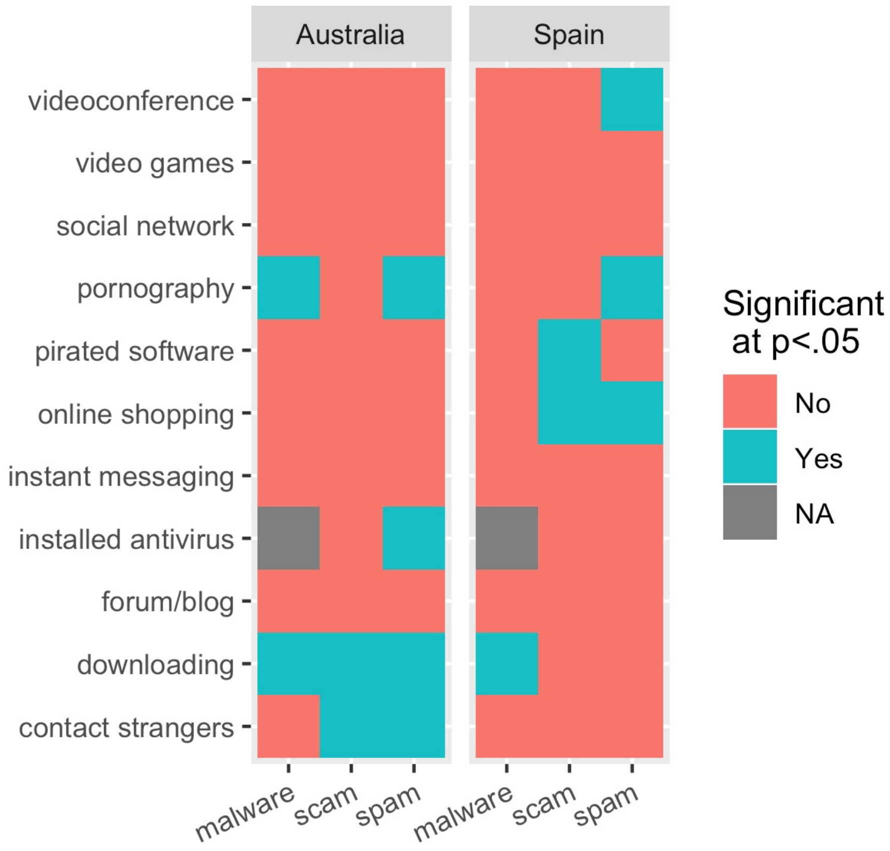
Table 3. Logistic Regression of Scam, Spam and Malware - Spanish Sample.

	Scam	Spam	Malware
contact strangers	0.999***(0.251)	0.753**(0.248)	0.500*(0.248)
downloading	0.509*(0.240)	0.464 (0.237)	0.258 (0.257)
forum/blog	-0.292 (0.253)	0.018 (0.248)	-0.348 (0.266)
instant messaging	0.593*(0.266)	0.703**(0.262)	0.390 (0.330)
installed antivirus	-0.218 (0.267)	-0.056 (0.262)	
online shopping	0.534*(0.222)	0.654**(0.219)	-0.254 (0.289)
pirated software	0.806*(0.314)	0.946**(0.311)	-0.229 (0.249)
pornography	0.166 (0.232)	-0.310 (0.233)	0.827*(0.410)
social network	0.262 (0.372)	0.644 (0.379)	0.680**(0.249)
video games	0.289 (0.488)	0.518 (0.490)	-0.038 (0.430)
videoconference	0.894***(0.262)	0.590*(0.256)	0.355 (0.334)
Constant	-1.913***(0.568)	-1.980***(0.568)	0.478*(0.242)
Nagelkerke R2	0.251	0.219	0.111
Observations	459	458	470
Log Likelihood	-48.002	-41.153	-17.846

Note: ⋆ = p<0.1; ⋆⋆ = p<0.05; ⋆⋆⋆ = p < .01
Coefficients are log odds.
Antivirus was not included for Malware model because the item used to determine this form of victimisation includes the use of antivirus software.

In Figure 3 we summarize all results by indicating which independent variables are observed to be statistically significant at the conventional .05 level.

Figure 3. Comparison of all model results by country



4.3.1. Spam victimization

For the Australian and Spanish samples, pornography use increased the risk of spam victimization. For the Spanish sample only, online shopping and videoconferencing increased risk of spam victimization. Increased spam victimization for the Australian sample associated with anti-virus software, downloading files and contact with strangers.

4.3.2. Scam victimization

For the Spanish sample only, online shopping and pirated software increased risk of spam victimization. For the Australian sample scam victimization was associated with downloading files and contact with strangers.

4.3.3. Malware victimization

For the Australian and Spanish samples, downloading files increased the risk of malware victimization. For the Australian sample malware victimization was also associated with pornography use.

4.3.4. Summary

In summary, participating in online forums/blogs, instant messaging, social networks and video games does not influence any victimization type for either sample. The current study indicates that for Spaniards online shopping is the riskiest type of activity, with increased risk for two out of three victimization outcomes (scam and spam). For Australians, downloading files is associated with increased risk of all victimization outcomes, making this the riskiest type of activity. Contact with strangers (scam and spam) and pornography use (spam and malware) is associated with increased risk of two of three victimization outcomes.

Discussion and Conclusion

The current study identified risk factors associated with the preparatory steps used by offenders. Fraudulent emails (victimization by scam and victimization by spam) and malicious software (victimization by malware) were conceptualized as some of the most commonly experienced types of approaches that are undertaken. It was argued that a greater understanding of preparatory attacks by offenders is necessary in order to intervene and disrupt subsequent cyber-attacks earlier in crime commission process. The study sought to identify online behaviors of potential victims that make them at increased risk of cybercrimes that target financial and/or personal information.

The current study found that Spain and Australia have similar prevalence rates for scam and spam victimization, with Spain experiencing elevated levels of malware victimization relative to the Australian sample. Across the samples, individuals engaged in similar proportions of many of the online behaviors that were studied (i.e. video games, pornography use, online shopping, instant messaging, forum/blog and downloading files).

The study found that the risk of experiencing spam, scam, and malware victimization does increase as a function of the amount of engagement that potential victims have online, however it is associated with specific types of activities in cyberspace. This study addresses limitations of much previous research that has failed to study differences across distinct types of cybercrime (Bergmann et al., 2018). Four out of the 11 online behaviors studied (online forums/blogs, instant messaging, social networks and video games) did not influence any victimization type in either Spain or Australia. As discussed in more detail later, specific types of online activities have different risk profiles. Engagement with different types of online activities does appear to differentially expose potential victims to subsequent victimization outcomes. These findings support and extend previous research that has found that target suitability and target visibility are strong correlates of victimization (Drew & Farrell, 2018; Hutchings & Hayes, 2008; Pratt et al., 2010). It provides further evidence that it is not only target visibility that needs to be understood, but the nuances of the types of activities that are enacted by potential victims (Reyns et al., 2018). This study has provided evidence to suggest that types of online behaviors are not only important to understanding victimization risk generally, but are relevant to understanding the likelihood of being a victim of a preparatory cyber-attack. The research demonstrates that a detailed understanding of preparatory attacks is needed. To develop maximally effective prevention and disruption efforts, we need to continue to study the relationship between different types of online activities and specific victimization outcomes (Bergmann et al., 2018).

This research indicates that education and disruption efforts, regardless of country of residence, should focus on the increased risk of downloading files. In Spain and Australia, downloading files is associated with both spam and scam victimization. Downloading files is a particularly risky activity for Australians, with this activity being associated with all three victimization outcomes (also, malware victimization). Further, in further pursuit of prevention and disruption efforts, individuals in both Spain and Australia need to be aware of the increased exposure to spam victimization that is associated with pornography use. In Spain specifically, the riskiest online behavior was online shopping with it related to two out of three victimization outcomes. This research confirms that need for victimization to be understood according to specific artefacts of target suitability and target visibility that are aligned with specific types of cyber crime activities and subsequent outcomes (Hutchings & Hayes, 2008; Pratt et al., 2010). This research demonstrates the utility of understanding risky behaviors (Choi, 2008).

In addition to the findings already discussed, depending on country of analysis, a number of online behaviors were differentially associated with victimization risk, installed antivirus with spam in Australia, pirated software with scam in Spain, and video conference with spam in Spain. These findings indicate that consideration should be given, at least in the context of preparatory attacks, to the country in which potential cybercrime victims reside. Whilst many when applying RAA in the context of cybercrime consider the concept of 'place' as generic cyber space, this research demands us to consider this generalization more carefully. One possible interpretation is that countries provide different attack surfaces, for example English-speaking countries are exposed to different internet environments, i.e., internet sites and hence, different groups of offenders. Research presented by Klavans (2015) indicates that not surprisingly English is the predominant language used on the Internet. It has been reported that in 2011, almost 40% of the Spanish-speaking world are using the Internet and using it in Spanish (it is acknowledged that not Spanish-speakers are located in the geographical borders of Spain where the current study was conducted) (Klavans, 2015).

Whilst the research has provided some interesting results, it is acknowledged that there are a number of weaknesses in the research design that should be addressed in future replication efforts. The construct of preparatory attacks needs to be further refined and robust measures need to be developed. Further, the victimization outcome measures were dichotomous. Future research should explore variation and dosage effects of victimization outcomes. In addition to addressing the limitations of the current study, future research should more actively employ research designs that draw samples from across countries. As highlighted earlier, while cyberspace has no borders and cybercrime is inter-jurisdictional in nature, we would be wise to not lose sight of the potential impact that traditional geographic borders may still have on the three key elements of crime: place (e.g. defined by language of internet sites), victims and offenders.

The current research was exploratory in nature, it introduced the concept of preparatory attacks and undertook this analysis across two geographically distinct sample populations. This research addressed an important gap in the literature by focusing on the effectiveness of protective behaviors that may be enacted by potential victims when they are targeted by these specific types of preparatory attacks. It provided evidence to support the contention that it may be possible to more effectively interrupt and prevent many types of subsequent cybercrimes that flow from these initial preparatory and harvesting methodologies. This may be done by gaining a better understanding of the relationship between online behaviors and preparatory attacks. This research has suggested that adopting a focus on the first possible crime prevention intervention point for many types of financial and identity exploitation crimes enacted in cyber space (scams, spam and malware) is a promising idea that needs further analysis. In the pursuit of more impactful education, prevention and law enforcement efforts to effectively disrupt the seemingly ever increasing, serious and devastating outcomes of cybercrime, research such as that undertaken in the current study is needed. Research needs to test new ideas and approaches and most importantly, research must consider the full range of intervention points that can be targeted at the earliest point in the crime commission process to reduce victimization rates and harm.

Acknowledgements

The authors acknowledge and thank Ms Kelsey Pruden, School of Criminology and Criminal Justice, Griffith University for her research assistance in the survey construction and data collection phases of the research.

References

Australian Cyber Security Centre (ACSC). (2017). *Threat report.* Retrieved from https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf.

Bangs, M. (2017). *Crime in England and Wales: year ending December 2017.* Statistical bulletin. Office for National Statistics. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2017.

Bergmann, M. C., Dreibigacker, A., vonSkarczinski, D. & Wollinger, G. R. (2018). Cyber-dependent crime victimization: The same risk for everyone? *Cyberpsychology, Behavior and Social Networking, 21(2),* 84-90.

Bossler, A. M. & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38,* 227-236.

Bossler, A. M. & Holt. T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3(1),* 400–420.

Caneppele, S., & Aebi, M. F. (2017). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice, pax055.* doi: 10.1093/police/pax055

Choi, K.S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2(1),* 308–333.

Cohen, L., & Felson, M (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588-608.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology, 21*(1), pp. 187-204

Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimization in Australia. *Trends & Issues in Crime and Criminal Justice*, *474.*

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research: An International Journal, 19(6),* 537-549.

Gupta, B. B., Arachchilage, N. A. G. & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunications Systems, 67,* 247-267.

Holt, T., & Bossler, A. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35,* 20-40.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses.* London, UK: Routledge.

Holt, T. J., & Bossler, A. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30(1),* 1-25.

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimization: who gets caught in the net. *Current Issues in Criminal Justice, 20,* 433-451.

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79.

Klavans, J.L. (2015). *Cybersecurity: What's language got to do with it?* Retrieved from https://drum.lib.umd.edu/bitstream/handle/1903/17165/LAMP-TR-158.pdf;sequence=1.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551-555.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37(3),* 263-280.

Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal justice review, 35*(4), 412-437.

McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice, 31,* 30–52.

Miró-Llinares, F. (2015). That Cyber Routine, That Cyber Victimization: Profiling Victims of Cybercrime. In, R. G. Smith, R. C. C. Cheung and L. Y. C. Lau (Eds.), *Cybercrime Risks and Responses* (pp. 47-63). London, UK: Palgrave Macmillan.

Miró-Llinares, F. (2011). La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología, 13*(7), 1-55.

Miró-Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons.

Miró-Llinares, F., & Johnson, S. D. (2018). Cybercrime and Place: Applying Environmental Criminology to Crimes in Cyberspace. In, G. J. N. Bruinsma & S. D. Johnson (Eds.), *The Oxford Handbook of Environmental Criminology* (pp. 883-906). Oxford, UK: Oxford University Press.

Miró-Llinares, F., Moneva, A., & Esteve, M. (2018). Hate is in the air! But where? Introducing an algorithm to detect hate speech in digital microenvironments. *Crime Science.* doi: 10.1186/s40163-018-0089-1

Ngo, F., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5(1),* 773-793.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine Online Activities and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency, 47(3),* 267–297.

Reyns, B. W. (2017). Routine activity theory and cybercrime: A theoretical appraisal and literature review. In K. F. Steinmetz & M. R. Nobles (Eds.), *Technocrime and criminological theory* (pp. 35–54). New York: Routledge.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal justice and behavior, 38*(11), 1149-1169.

Statista. (2018). Global spam volume. Retrieved from https://www.statista.com/statistics/420391/spam-email-traffic-share.

United Nations. (2016). *The state of broadband: Broadband catalyzing sustainable development. Broadband Commission for Sustainable Development.* Retrieved from http://www.broadbandcommission.org/Documents/reports/bb-annualreport2016.pdf.

US Internet Crime Complaint Center (IC3). (2018). *Internet crime report.* Retrieved from https://pdf.ic3.gov/2018_IC3Report.pdf.

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice, 32,* 169–188.

Van Wilsem, J. (2013). 'Bought it, but never got it' Assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168-178.