Güvenlik Bilimleri Dergisi, Mayıs 2020,Cilt:9 Sayı:1, 243-268 *DOI:10.28956/gbd.736179*

CARD-NOT-PRESENT FRAUD VICTIMIZATION: A ROUTINE ACTIVITIES APPROACH TO UNDERSTAND THE RISK FACTORS

Naci AKDEMIR*, Serkan YENAL**

Abstract

Banking cards, including credit cards, debit card, pre-paid debit cards and ATM cards, have become the primary payment method in online transactions. However, this popularity boosted the Card-not-present (CNP) fraud victimization. Despite numerous studies exploring technological solutions to prevent CNP fraud, there is a shortage of theoretically informed research exploring the online lifestyle correlates of CNP.

This study, which utilizes the dataset of Crime Survey for England and Wales 2014/2015, addresses this gap in the literature. Routine Activities Theory was used as the theoretical and conceptual framework in this present study. Bivariate and multivariate analyses results suggested that home users' online lifestyle increases the risk of becoming a victim of CNP fraud. Buying goods or services, accessing online government services and online communication (email/instant messaging and chat rooms) emerged as risk factors. Illustrating the impact of technological vulnerabilities (mobile phones and public access computers) on the risk of CNP fraud victimization was another novel contribution of this study.

Additionally, personal guardianship measures, using complex passwords and different passwords, emerged as predictors of victimization. These results provide valuable implications for situational crime prevention efforts. Practical and theoretical implications of this study are further discussed.

Keywords: *Card-Not-Present Fraud, Fraud, Cybercrime, Identity Theft, Situational Crime Prevention, Routine Activities Theory, Security, International Relations*

ÇEVRİMİÇİ BANKA KARTI DOLANDIRICILIĞI: RİSK FAKTÖRLERİNİ ANLAMADA RUTİN AKTİVİTELER YAKLAŞIMI

Öz

Kredi kartları, banka kartı, ön ödemeli banka kartları ve ATM kartları dahil olmak üzere banka kartları, çevrimiçi işlemlerde öncelikli ödeme yöntemi haline gelmiştir. Ancak bu popülerlik banka kartlarının fiziksel olmayan kullanımı dolandıcılığı (BKFOK) mağduriyetinin artmasına neden olmuştur. BKFOK dolandırıcılığını önlemek için teknolojik çözümleri araştıran çok sayıda çalışmaya rağmen, BKFOK dolandırıcılığının çevrimiçi yaşam tarzı ilişkilerini araştıran teorik olarak temellendirilmiş araştırma eksikliği mevcuttur.

İngiltere ve Galler 2014/2015 Suç Araştırması veri setininin kullanıldığı çalışmamız, literatürdeki bu boşluk üzerinde kurgulanmıştır. Bu çalışmada teorik ve kavramsal çerçeve olarak Rutin Aktiviteler Teorisi kullanılmıştır. İki değişkenli ve çok değişkenli analiz sonuçları, ev kullanıcılarının çevrimiçi yaşam tarzının BKFOK Dolandırıcılığı kurbanı olma riskini artırdığını göstermektedir. Çevrimiçi mal veya hizmet satın almak, çevrimiçi devlet hizmetlerine erişmek ve çevrimiçi iletişim (e-posta / anlık mesajlaşma ve sohbet odaları) risk faktörleri olarak ortaya çıkmıştır. Teknolojik güvenlik açıklarının (cep telefonları ve kamusal alanda kullanılan açık erişim bilgisayarlar) BKFOK dolandırıcılığı mağduriyeti riski üzerindeki etkisini ortaya koymak, bu çalışmanın bir başka önemli katkısıdır.

Buna ek olarak, karmaşık parolalar ve farklı parolalar gibi bireysel güvenlik tedbirlerini kullanmak mağduriyetin tahminleyici faktörleri olarak ortaya çıkmıştır. Bu sonuçlar durumsal suç önleme çabaları için değerli sonuçlar vermektedir. Bu çalışmanın pratik ve teorik sonuçları metin içerisinde tartışılmaktadır.

Anahtar Kelimeler: *Banka Kartı Dolandırıcılığı, Dolandırıcılık, Siber Suçlar, Kimlik Hırsızlığı, Suç Önleme, Rutin Aktiviteler Teorisi, Güvenlik, Uluslararası İlişkiler*

* Dr. Öğr. Görevlisi, Jandarma ve Sahil Güvenlik Akademisi, naciakdemir@jandarma.gov.tr, ORCID: 0000-0002-4288-6482

** Dr. Öğr. Üyesi, MSÜ KHO Svn. Yön. Bölümü, syenal@kho.edu.tr, ORCID: 0000-0002-8188-5095

Makale Geliş Tarihi: 14.04.2020 Makale Kabul Tarihi: 27.04.2020

INTRODUCTION

The rapidly developing technology and the new world order have changed the habits of the people. Especially since the second half of the 1990s when the Internet started to become widespread, significant changes have occurred in shopping habits. The traditionally face-to-face business activities have evolved rapidly and began to be carried out over the Internet. While electronic commerce has changed old habits, it has increased its trade volumes and enabled many businesses to reach customers that they could not have imagined before. Those who could keep up with this change benefited from these advantages, while those who did not keep up lost their trade volume. E-commerce, which is the trade of goods, products and services over the Internet (Turban et al., 2017), is one of the fastest-growing industries in the world (Shabir, Hamad, and Anosh, 2014). EMarketer estimates that e-commerce sales have reached $ 3.538 trillion, which accounted for 14,1% of global trade. It is forecasted that e-commerce sale will approach $ 5 trillion in 2021 (17,1% of all sales) (Lipsman, 2019).

The prevalence of e-commerce has boosted the popularity of banking cards use dramatically. Over the past ten years, credit cards have become the most preferred payment method.(Turban et al., 2017). For example, credit card payments accounted for 75% of all spending of the retail sector in the UK, which makes the UK biggest credit card payment market in Europe. However, this growth in e-commerce and banking card sector is not free from its problems. Card-not-present fraud has become an essential issue in e-commerce due to increased volumes of CNP fraud incidents. According to the Federal Trade Commission report, approximately 158.000 credit card fraud cases reported, accounting for 29% of all reported cases (FTC, 2019).

In response to emerging threats of fraud activities, security-enhanced practices for individuals and institutions have been devised over time. Numerous protection mechanisms for this purpose have been developed on credit cards and websites. These include measures such as limiting online shopping limits, creating additional password mechanisms, virtual card applications, the introduction of the chip and technology and EMV (Europay, Mastercard and Visa) standards. Although these measures provided significant protection, credit card fraud on the Internet could not be terminated entirely. While the measures are increasing and diversifying, fraudsters adapt to them and always find new methods.

Card-not-present (CNP) fraud, which can be defined as unauthorized use of payment cards in the absence of a physical payment card (Montague, 2010), has become an emerging threat over the last years. However, despite the significant threat posed by CNP fraud, there is a lack of empirical research on the causes of CNP fraud. Most of the studies(e.g. Branco et al., 2020; Mittal and Tyagi, 2020; Singh and Jain, 2020) have dealt with technical and technological solutions to CNP fraud. This study aimed to address this gap in the literature by exploring the online lifestyle determinants of CNP fraud through bivariate and multivariate analysis of Crime Survey for England and Wales 2014/2015. Routine Activities Theory (RAT) is utilized as a theoretical and conceptual framework while examining the lifestyle factors that facilitate CNP fraud victimization.

1. LITERATURE REVIEW

1.1 Typology of Card-not-present (CNP) Fraud

CNP fraud has two distinct attributes, being a hybrid and output crime. Wall (2007) classifies frauds as a hybrid cybercrime since frauds can be committed in both cyberspace and the real world. CNP fraud can be regarded as a hybrid cybercrime since perpetrators can obtain credit card information through skimming and scanning of physical cards in the real world. Additionally, offenders may persuade users to yield credit card credential via socially engineered unsolicited emails in cyberspace (Akdemir, Sungur and Basaranel, 2020).

Moreover, Wall (2007) conceptualizes three generations of cybercrimes. Whereas the first-generation cybercrimes act as a secondary or tertiary tool to assist conventional crimes such as bank robbery, the second-generation cybercrimes create new opportunities for perpetrators (e.g. enabling fraudsters to access personal information of a person who lives in another country). The third-generation cybercrimes are those that could only be committed in cyberspace; for instance, spamming can only be committed via networked technologies. Based on this classification, card-not-present fraud can be considered as a second-generation cybercrime since the Internet created numerous opportunities for fraudsters such stealing card details via infected computers or selling stolen credit card detail in online black markets (Thomas, Thiry, Hsu, Traver, and Tengkiattrakul, 2014; Bulakh and Gupta, 2015).

Furthermore, card-not-present fraud may also be considered as an output cybercrime since it requires the use of illegally obtained credit card details over the

Internet or telephone. Card-not-present fraud, rather than being a result of one single event, is an outcome or the last stage of a process (Howard, 2009). The process begins with input activity, such as identity theft, or physically loss of cards and ends with card-not-present fraud, which encompass cashing out the money or goods. The first stage of this process is the main focus of this study since victims' actions or lifestyle may facilitate the fraudulent process, which is named as victim facilitation (Smith, Bouffard, and Justice, 2014). This study specifically examines the victims' contributions to their victimization through their online lifestyles.

Online Fraud Victimization

Online fraud victimization (Holtfreter, Reisig, and Pratt, 2008; Pratt, Holtfreter, and Reisig, 2010; Button, Nicholls, Kerr, and Owen, 2014), credit card theft victimization (Reisig, Pratt, and Holtfreter, 2009), online advertisement fraud (Garg and Nilizadeh, 2013) online dating scams (Rege, 2009) and online consumer fraud victimization (van Wilsem, 2011) are the types of online frauds to be reviewed here.

Several online victimization studies thus far have linked victims' online activities with online fraud victimization (Reisig et al., 2009; van Wilsem, 2011; Button et al., 2014). Spending more time on the Internet to shop goods, checking online forums and having profiles on different social media websites (Pratt et al., 2010; van Wilsem, 2011), remote online purchasing (Holtfreter, Reisig, Leeper Piquero, and Piquero, 2010; Reyns, 2013), responding dating scams (Rege, 2009), online social activities (i.e. using chatrooms, visiting Internet forums) (Marcum, Higgins, and Ricketts, 2010; van Wilsem, 2011, 2013b) and Internet banking (Hutchings and Hayes, 2008; Reyns, 2013; Reyns, 2015) were associated with the increased risk of online fraud victimization.

Previous research has indicated that various demographic indicators have a significant impact on online fraud victimization. Age (Pratt et al., 2010; Ngo and Paternoster, 2011; van Wilsem, 2011; Leukfeldt and Yar, 2016), gender (Holtfreter et al., 2008; Garg and Nilizadeh, 2013; Holt, 2013; Choi, Choo, and Sung, 2016), marital status (Pratt et al., 2010), educational level (Pratt et al., 2010; van Wilsem, 2011, 2013a, 2013b; Paek and Nalla, 2015), were correlates of online fraud victimization. Annual household income was also associated with an increased risk of victimization. Empirical evidence suggested that Internet users' with higher annual household income were more likely to be a victim of cybercrime (Pratt et al., 2010; van Wilsem, 2011, 2013a, 2013b; Paek and Nalla, 2015). Additionally, Schoepfer and Piquero (2009) found that age was a negative predictor of credit card fraud, which means that young people are at the increased risk of being the victim of credit card fraud.

Although some fraud victimization studies researched credit card fraud victimization within the general context of fraud victimization(Bossler and Holt, 2009; Schoepfer and Piquero, 2009) only Reisig et al. (2009) studied credit card fraud victimization in separate research. Reisig et al. (2009) studied the effect of impulsivity and perceived risk of credit card theft victimization on online behaviors. They conducted a telephone survey in Florida with 573 adult participants. Online purchasing and the amount of time spent online were the online behaviors that were under examination. They have found that those with the high level of perceived risk of victimization avoided online purchasing and they decreased the time spent online. Yet, impulsive respondents did not alter their online behaviors. Individuals who belong to an ethnic minority and with lower socio-economic status were more prone to have high levels of risk perception.

2. THEORETICAL FRAMEWORK

Although Wolfgang conducted the first victimization studies in the 1950s (Wolfgang and Science, 1957), it was after the introduction of two ground-breaking victimization theories, Lifestyle-exposure (Hindelang, Gottfredson, and Garofalo, 1978) and Routine Activities Theory (Cohen and Felson, 1979) that victimization and the role of the victim in the occurrence of crime received considerable attention (Meier and Miethe, 1993). The intention of the two aforementioned theories is to offer a systematic approach to explain victimization rather than blaming victims. Opportunity theories, namely Routine Activity Theory and Lifestyle-Exposure theory, shifted the attention from the offending behavior to victims' lifestyle and routine activities, which proposed to prepare suitable conditions for crime. This approach was a real challenge for criminologist who sought remedy in examining the offending behavior (Miethe and Meier, 1994). Routine Activities perspective postulates that the motivated offender, the suitable target and the absence of capable guardian are three minimal elements for a crime to occur (Hindelang et al., 1978; Cohen and Felson, 1979). Namely, these elements are necessary conditions for a crime to occur; hence controlling these conditions may prevent victimization (Miethe and Meier, 1990; Mustaine and Tewksbury, 1998).

Exposure and Proximity to Motivated Offender: Whereas exposure refers to "physical visibility and accessibility" of victims, proximity refers to "physical distance" between motivated offender and victims (Cohen, Kluegel, and Land, 1981, p. 507). Due to the nature of the cyberspace, victims do not expose themselves to the perpetrators physically. Thus, there is no physical distance between offenders and victims in the online environment. However, victims are in close proximity to offenders' tools rather than physical existence (Holt and Bossler, 2016); hence, the proximity to the motived offender is zero in the Cyberspace (Yar, 2005). Whereas victims mostly expose themselves to the offenders in conventional street crimes, victims usually disclose their personal information to the perpetrators in cyberspace. The Internet users' online behaviors and lifestyles increase the exposure to the motivated offender and put themselves in closer proximity to motivated offenders' tools (Holt and Bossler, 2013).

Suitable Target: Cohen and Felson (1979)) argue that some specific features of a target value, inertia, visibility and accessibility, known as VIVA, increase the target attractiveness. Later Clarke (1995) based on these characteristics of a target, created a model called CRAVED, concealable, removable, available, valuable, enjoyable and disposable. (Clarke and Felson, 1998) dubbed the targets that have these qualifications as "hot products", which are the items that are mostly preferred by thieves. These hot products can be cars, jewellery or money in the real world; however, the hot product of cyberspace is information such as credit card numbers (Newman and Clarke, 2013). Since the target attractiveness of personal data is high in the online environment, fraudsters seek suitable targets in cyberspace and Internet users' some of the online behaviors and online lifestyle increase target suitability (Holt and Bossler, 2013).

Absence of a Capable Guardian: Cohen et al. (1981) define guardianship as the capability of the persons or things to prevent crime. Whereas the guardians in the real world can be police officers, family members or alarms, the guardians in cyberspace are anti-virus programs, firewalls, or personal security measures such as checking the security signs of a website.

Lifestyle Exposure Theory (Hindelang et al., 1978) assumes that changes in crime rate may be attributed to the victims' demographics, which causes differences in lifestyles (Miethe, Stafford, and Long, 1987; Sampson and Wooldredge, 1987). Risky lifestyles lead individuals to engage in activities that increase the risk of victimization. Later, Cohen et al. (1981) implicitly combined two theories in their research, and since then, these two theories have been used in tandem. Lifestyle Routine Activities theory (LRAT) has been applied to explain different kinds of victimization: violent victimization(Bouchard, Wang, and Beauregard, 2012), sexual assault (Fisher, Daigle, and Cullen, 2010) burglary victimization (Cohen and Cantor, 1981; Kennedy and Forde, 1990; Miethe and McDowall, 1993) are only a few examples of the huge amount of victimization studies that applied LRAT as the theoretical framework. It was (Grabosky), 2001) who initially proposed that Routine Activities Theory might be applicable to online crimes. Since then, the LRAT perspective has been widely used in cybercrime studies.

3. PRESENT STUDY

CNP fraud is the unauthorized use of banking cards' information, while the physical card is not present (Montague, 2010). Precautions applied to prevent skimming and scanning of the physical card as well as the increased volume of online transactions have motivated online offenders to devise new strategies to acquire Internet users' payment card information (Wall, 2010; Reyns and Henson, 2016). The extant research on the payment methods mainly focuses on the factors affecting customers' payment method choice (i.e. Ching and Hayashi, 2010; See-To, Papagiannidis, and Westland, 2014; Arango, Huynh, and Sabetti, 2015) and technical solutions to reduce the risk of financial loss through online attacks (i.e. Sendo, Sherman, and Kaltwasser, 2005; Ahmad, Zeki, and Olowolayemo, 2016; Vishal and Johari, 2018). Only a handful of studies have researched the correlates of card-not-present fraud.

Past empirical studies, which generally examined the relationship between low-self-control and credit card fraud victimization, yielded inconsistent results with regards to the relationship between low-self-control and CNP fraud victimization. Bossler and Holt (2010) who explored the impact of self-control on the various forms of cybercrime victimization, found no association between low-self-control and credit card information theft. However, Pratt et al. (2010) found that Internet users with low-self-control were more likely to be a victim of credit card fraud due to engaging with risky online activities which increased their exposure to perpetrators. Holtfreter et al. (2008) researched a different aspect of card-not-present fraud victimization. They investigated the impact of online credit card fraud victimization on online behavioral adaptation. The research results indicate that financially impulsive respondents were less likely to limit their online actions, which in turn increased the risk of victimization. Another study researching the behavioral impact of credit card fraud victimization showed that credit card fraud victims were less likely to use online payment methods (Kahn and Liñares-Zegarra, 2016).

This present study examines the online lifestyle correlates of CNP fraud victimization. To that end, three hypotheses were tested.

Hypothesis 1: Home users' online activities increase their exposure to the motivated offender, thereby increases the risk of CNP fraud victimization.

Hypothesis 2: High risk-electronic devices (laptop used away from secure Internet connections, smartphones and public access computers) increases the risk of CNP fraud victimization.

Hypothesis 3: Online safeguarding measures decrease the risk of CNP fraud victimization.

4. METHOD

4.1. Data

This study utilized the Crime Survey for England and Wales (2014/2105) (CSEW) (Office for National Statistics, 2020) to address the research questions: *"What are the online lifestyle correlates of CNP fraud victimization "*CSEW measures the extent of the crime in England and Wales. The survey, which is known as the British Crime Survey (BCS), has been conducted yearly since 2001. The survey recruited 35.000 adult participants living in England and Wales.

4.2. Measures

4.2.1 Dependent Variable

Card-not-present (CNP) Fraud Victimization: CNP fraud is defined as the unauthorized use of payment cards in the absence of a physical payment card. Survey asked the respondents: "*Have any of your cards been used* ***without your permission or prior knowledge*** *to take money from your bank or building society accounts or to charge money to your bank, debit, credit or store cards?"* The variable is coded dichotomously (0 = No, Yes = 1).

4.2.2. Independent Variables

Exposure to motivated offenders: RAT argues that people's routine daily activities increase their exposure to would-be offenders, thereby increasing the risk of victimization. Hence, online activities: (1) buying goods or services, (2) online banking or managing finances, (3) online government services, (4) email, instant messaging, chat rooms, (5) social networking, (6) browsing for news or information (7) playing online games/doing quizzes/competitions were operationalized as exposure to the motivated offender. Online behaviors, buying goods online, online banking and online government service usage, were conceptualized as high-risk online activities since these activities require disclosure of personal and financial information.

Target Suitability: This study proposed that electronic devices utilized to access the Internet may increase users' target suitability since technological vulnerabilities of these devices may be exploited to acquire individuals' credit card information. While variables (1) laptop (away from home and work or school/college), (2) mobile phone or smartphone, (3) handheld computer (e.g. iPad, tablet, palmtop) and (4) public access computer (e.g. In a library, internet cafe) were operationalized as high-risk electronic devices; (1) desktop computer (at home or work or school/college) and (2) laptop (at home or work or school/college) were operationalized as low-risk electronic devices.

Absence of capable guardianship: RAT perspective proposes that a capable guardian may prevent victimization. Previous cyber victimization research conceptualized online guardianship as digital and personal guardianship measures. Thus, this study operationalized (1) downloading software updates and patches whenever prompted, (2) only downloading known files or programs, (3) installing anti-virus or other security software, such as a firewall and (4) scanning computers regularly for viruses or other malicious software as digital guardianship measures. Additionally, (1) using of complex passwords (containing letters, numbers and symbols), (2) using a different password for each separate online account, (3) deleting suspicious emails without opening them,(4) only using well-known or trusted sites, (5) checking for signs that a site is secure before buying online were operationalized as personal guardianship measures.

5. ANALYTIC STRATEGY

This research conducted bivariate and multivariate analysis to address the research question and to test research hypotheses. The relationships between online lifestyle measures and CNP fraud victimization were measured via contingency tables. Pearson's chi-square test was used to assess the significance of the associations statistically since all variables were categorical (Field, 2009). The default significance level of 0.05 (α=0.05) was set as the threshold for testing the hypothesis through chi-square test since this significance level is more suitable for testing hypotheses (Payton, Greenstone, and Schenker, 2003). Phi test values were also obtained to observe the strength of the relationships. Whereas values from 0.00 to 0.10, referred to a weak association, values ranging from 0.11 to 0.30 denoted moderate association between binary variables and values greater than 0.30 referred to a strong association(Healey, 2014).

Multivariate analysis was conducted to assess the impact of each variable on the risk of experiencing CNP fraud victimization. Since the response variables were dichotomous categorical variables, namely variables with two categories, binary logistic regression analysis was conducted. Prior to conducting regression analysis, Variation Inflation Factor (VIF) scores were obtained to check the multicollinearity between response variables. Since the VIF test scores ranged between 1.004 to 1.276, there was no multicollinearity between predictor variables. Due to a large number of independent variables Backward Wald stepwise entry method was chosen during the analysis to obtain the model that fits the data best (Ho, 2013).

6. RESULTS

6.1. Bivariate Analysis Results

The relationships between Internet users' online behaviors (exposure to the motivated offender), target suitability (the type of electronic device used to access the Internet), online safeguarding measures and CNP fraud victimization were examined through bivariate analyses. Chi-square and Phi test results are reported in Table 1. Regarding exposure to the motivated offender, nearly all variables statistically significantly associated with CNP fraud victimization. Only, playing online games/doing quizzes/competitions (χ^2 =2.375, p$\geq$0.05) was not statistically significantly related to CNP fraud victimization. Likewise, all proxy measures of target suitability except for accessing the Internet via a laptop at home or work/school/college (χ^2 =2.852, p$\geq$0.05) were statistically significantly associated with CNP fraud victimization. Lastly, online guardianship measures excluding downloading software updates and patches whenever prompted (χ^2 =2.269, p≥0.05) and scanning computers regularly for viruses or other malicious software (χ^2 =2.541, p≥0.05) emerged as statistically significant correlates of CNP fraud victimization.

However, the Phi& Cramer's tests measuring the strength of these associations suggested that aforementioned relationships were weak since the Phi (θ) values were close to zero (Dytham, 2011; Jackson, 2013). This result indicates these relationships may disappear when other uncontrolled variables are included in multivariate analysis. Variables that were not statistically significantly associated with CNP fraud victimization were excluded from the binary logistic regression model.

6.2. Multivariate Analysis Results

Binary logistic regression analysis was conducted to discern the factors that render home users vulnerable to CNP fraud victimization (Table 2). Regarding the impact of online activities on the risk of becoming a victim of CNP fraud, buying goods or services online (Internet shopping, inc. music/film downloads), accessing the Internet for online government services, using e-mail, instant messaging, chat rooms emerged as statistically significant predictors of CNP fraud victimization. Results indicate that purchasing goods or services online has the most significant impact on the chances of becoming a victim. While holding other variables constant, home users who accessed the Internet mainly for online shopping were 87% more likely to be a victim of CNP fraud when compared to those who did not make online purchases (b=0.639, p ≤0.01, Exp. (B) =1.878). Likewise, users who utilized the Internet for online communication (e.g. e-mail/instant messaging/chat rooms) were at approximately 1.7 times more likely to be a victim of CNP fraud (b=0.388, p ≤0.05, Exp. (B) =1.474).

Furthermore, high-risk electronic devices (mobile phone or smartphone and public access computers) predicted CNP fraud victimization. Whereas accessing the Internet via mobile phone or smartphone enhanced the risk of victimization by approximately 44% (b=0.363, p ≤0.01, Exp. (B) =1.438), using public access computers increased the likelihood of becoming a victim by nearly 37%(b=0.314, p ≤0.05, Exp. (B) =1.369).

Table-1 *Bivariate Analysis Results*

	Card-not-present Fraud	
	Phi	*Chi-square Tests*
Exposure to Motivated Offender		
Online banking or managing finances (e.g. paying credit cards)	*0.057*	*19.946****
Buying goods or services (internet shopping, inc. music / film downloads)	*0.068*	*28.305****
Online government services (e.g. tax returns, DVLA, council tax, benefits)	*0.071*	*30.171****
Social networking (e.g. Facebook, Twitter) or blogging	*0.039*	*9.346***
E-mail, instant messaging, chat rooms	*0.052*	*16.234****
Browsing for news or information (e.g. BBC, Wikipedia)	*0.033*	*6.685***
Playing online games/doing quizzes/competitions	*0.021*	*2.375*
Target Suitability		
Low Risk Electronic Devices		
Desktop computer (at home or work or school/college)	*0.031*	*5.699***
Laptop (at home or work or school/college)	*0.022*	*2.852*
High Risk Electronic Devices		
Laptop (away from home and work or school/college)	*0.045*	*12.258****
Mobile phone or smartphone	*0.052*	*16.728****
Handheld computer (e.g. iPad, tablet, palmtop)	*0.051*	*15.436****
Public access computer (e.g. In a library, internet cafe)	*0.031*	*5.458***
Online Guardianship		
Only downloaded known files or programs	*0.033*	*6.695***
Downloaded software updates and patches whenever prompted	*0.019*	*2.269*
Used complex passwords (contain letters, numbers and symbols)	*0.031*	*5.909***
Used a different password for each different online account	*0.037*	*8.309***
Deleted suspicious emails without opening them	*0.048*	*14.011****
Installed anti-virus or other security software, such as a firewall	*0.041*	*9.896***
Scanned computer regularly for viruses or other malicious software	*0.042*	*9.812***
Only used well-known or trusted sites	*0.021*	*2.541*
Checked for signs that a site is secure before buying online	*0.031*	*5.782***

*=p ≤0.05 **=p ≤0.01 ***=p ≤0.001

Table-2 *Binary Logistic Regression Analysis*

	Card-not-present Fraud		
Variables in the Equation	*B*	*S.E.*	*Exp(B)*
Exposure and Proximity to Motivated Offender			
Buying goods or services (Internet shopping, inc. music/film downloads)	0.630	0.244	1.878**
Online government services (e.g. tax returns, DVLA, council tax, benefits)	0.388	0.153	1.474**
E-mail, instant messaging, chat rooms	0.525	0.271	1.691*
High-Risk Electronic Devices			
Mobile phone or smartphone	0.363	0.158	1.438**
Public access computer (e.g. In a library, internet cafe)	0.314	0.173	1.369*
Online Guardianship			
Used complex passwords (contain letters, numbers and symbols)	-0.255	0.148	0.775*
Used a different password for each different online account	0.265	0.128	1.303**
Constant	-4.447	0.298	0.012***

*=p ≤0.05 **=p ≤0.01 ***=p ≤0.001

Lastly, two online safeguarding measures (using complex passwords and using different passwords for each different online account) emerged as statistically significant predictors of CNP fraud victimization. Home users who used complex passwords which contain letters, numbers and symbols were less likely to be a victim. Utilizing complex passwords decreased the risk of victimization by 22.5% (b=0.388, p ≤0.05, Exp. (B) =0.775). However, using different passwords for different online accounts increased the odds of becoming a victim. Internet users who preferred to use different passwords for online accounts were 30% more likely to be victimized when compared to those you used the same password for different online accounts. This result is counter-intuitive since it was expected that using different passwords may reduce the risk of victimization. Implications of these results will be discussed in the following Discussion section.

7. DISCUSSION

The widespread use of the Internet created many trading opportunities for both companies and individuals due to the borderless nature of the cyberspace. Remote purchasing is one of the various novelties of cyberspace. Due to the ease of use, credit cards have become the primary payment method in online transactions. However, after the introduction of new security measures such as chip and pin and EMV (Europay, Mastercard, Visa) online perpetrators devised new methods to exploit users' vulnerabilities to gain access to credit card information (Wall, 2010; Anderson and Murdoch, 2014). Despite the growing body of research examining the causes of cybercrime victimization such as online banking fraud (Jansen and Leukfeldt, 2015; Jansen and Van Schaik, 2018) and identity theft (Holt and Turner, 2012; Reyns, 2013; Jordan, Leskovar, and Marič, 2018), the causes of CNP fraud victimization remained relatively unexplored. This empirical study aimed to address this gap in the literature. To that end, three hypotheses were tested. Routine Activities Theory (RAT) is utilized as a theoretical and conceptual framework while examining the determinants of CNP fraud victimization. Backwards binary logistic regression analysis was conducted to test the impact of each variable on the risk of experiencing CNP fraud victimization.

RAT proposes that individuals' routine activities and lifestyles create criminal opportunities (Cohen and Cantor, 1981). Individuals who are more exposed to potential offenders would be at increased risk of victimization (Hindelang et al., 1978). Following this line of logic, it was hypothesized that high-risk online activities (purchasing goods online, using online banking and accessing online government services) would increase the risk of victimization since these activities require disclosure of personal identifying and financial information (H1). Analysis result yielded support for this proposition. Two of the three high-risk online activities emerged to enhance the likelihood of CNP fraud victimization. This result is in line with prior cybercrime victimization studies suggesting online shopping as a risk factor (Pratt et al., 2010; Reyns, 2013). Illustrating the impact of online government service usage on the risk of CNP fraud is the novel contribution of this study. This study, for the first time, demonstrated that online government websites enhance the chance of CNP fraud. This result could be attributed to bogus websites mimicking online government websites (Akdemir, 2019).

Additionally, accessing the Internet for online communication also emerged as a risk factor. Prior research demonstrated that perpetrators conduct online romance scams, which mainly used instant messaging and chat rooms as a mean of communication, to obtain credit card and other financial information of Internet users(Cross, Richards, and Smith, 2016; Gillespie and Magor, 2020). Internet users who reported CNP fraud victimization might be defrauded through dating scams.

Target suitability is another construct of RAT. It is argued that some attributes of individuals render them suitable targets for potential perpetrators (Hindelang et al., 1978; Miethe and Meier, 1994). It is argued that individuals sharing some common demographic characteristics are more likely to be a target of a crime. Younger age (Ngo and Paternoster, 2011; Choi et al., 2016; Leukfeldt and Yar, 2016), females (Holt and Bossler, 2013) and higher socioeconomic status (Pratt et al., 2010; van Wilsem, 2013a) were associated with increased risk of cybercrime victimization. This study included demographic characteristics (age, gender, income and education level) as control variables. However, none of the demographic variables remained in the final model of backwards binary logic regression. These results indicate the absence of demographic differences in CNP fraud victimization.

This study hypothesized high-risk electronic devices (mobile phones/smartphones, tablets and public access computer) would increase the risk of victimization (H2). Analysis result supported this proposition since two of the three variables measuring target suitability were associated with increased risk of CNP fraud. This finding is another novel contribution of this research. It appears that online perpetrators exploit the technological vulnerabilities of mobile devices. Lack of digital guardianship may be a reason for mobile phones being a risk factor. Whereas most people secure their personal computers with anti-virus software, a small proportion of users secure their mobile devices, which render these devices vulnerable to online threats (Kokh, 2019). Hence, unprotected mobile devices could be exploited to compromise personal and financial information.

Lastly, RAT argues that the presence of a capable guardianship may deter victimization (Cohen and Felson, 1979). This study hypothesized that online safeguarding measures would diminish the risk of CNP fraud victimization. However, multivariate analysis result yielded partial support to this proposition since none of the digital guardianship measures (installing security software, scanning computers regularly or downloading software updates) emerged as statistically significant predictors of CNP fraud. Only two password management strategies (using complex passwords and different passwords for online accounts) predicted victimization. Nevertheless, using complex passwords appeared to increase the risk of victimization. This unexpected result may be attributed to password fatigue, which refers to being overwhelmed with various passwords associated with multiple online accounts (Corre, Barais, Sunyé, Frey, and Crom, 2017). Cross-sectional nature of survey data could be another explanation for this results since previous cyber victimization studies also yielded similar counter-intuitive results (Ngo and Paternoster, 2011; Reyns, Henson, Fisher, Fox, and Nobles, 2016).

7.1. Practical Implications

The analysis revealed that remote purchasing and accessing online government services enhanced the likelihood of becoming a victim of CNP fraud victimization. This result suggests that home users should be wary of bogus websites. There are several ways of differentiating between fake and genuine sites. Green padlocks, website privacy policies and trust seals are the examples of these precautions. Users may also conduct a web search to find out issues related to online traders. Customer complaint centers and forums and blogs sometimes provide valuable information about online merchants. Public access computers such as those offered in libraries or Internet cafes emerged as significant risk factors for CNP fraud victimization. Since it is hard to monitor all individuals who accessed these computers, Internet users may abstain from utilizing these computers for financial activities such as online shopping. Lastly, due to ease of use, mobile devices are largely used to shop online. Though most of the users secure their computers with security software, mobile devices remain relatively under-protected. The results of this study suggest that either mobile devices should be protected well or the use of these devices in online financial activities be limited. Home users should be aware of the risks mobile devices pose.

7.2. Research Implications and Limitations

This study illustrated that high-risk online activities, which require users to reveal their personal and financial information, poses significant risks for CNP fraud victimization. However, due to unavailability of questions measuring the impact of online deviant activities such as illegal downloading, peer-to-peer sharing or free streaming, this study could not explore the effect of online deviance on the likelihood of becoming a victim of CNP fraud. Future research may explore the relationship between CNP fraud and online deviance. Moreover, digital guardianship measures did not predict CNP fraud victimization. Future research may consider exploring the capable guardians of CNP fraud.

CONCLUSION

This study examined the online lifestyle correlates of a relatively unexplored area of CNP fraud victimization. Three hypotheses tested the constructs of Routine Activities Theory (RAT), exposure to the motivated offender (H1), target suitability (H2) and online guardianship (H3) through a nationally representative sample of Crime Survey for England and Wales (CSEW 2014/2015). Analyses results yielded support to hypothesis 1 and hypothesis 2. This result is in line with previous research (Pratt et al., 2010; Ngo and Paternoster, 2011; Reyns, 2013; Choi et al., 2016) testing the applicability of these two constructs to cybercrime victimization. However, the results handed partial support to the third hypothesis, which proposed that online guardianship measures would decrease the risk of CNP fraud victimization. Furthermore, the counter-intuitive result indicating complex password usage as a risk enhancing factor was another issue related to hypothesis 3. Yet, this result confirms previous cyber victimization studies (e.g. Ngo and Paternoster, 2011 and Reyns et al., 2016). Overall, it can be argued that the analysis results supported initial hypotheses, and the finding of the research is in line with existing research.

The situational crime prevention approach proposes that crimes can be prevented or reduced should the conditions and opportunities that lead to victimization be controlled or reduced (Clarke, 1980). The idea of "highly specific forms of crime" is at the heart of this perspective (Clarke, 1995, p. 93). This means that the success of this approach lies in focusing on specifications of every type of crime individually. Hence, this research focused on discerning the factors that render home users vulnerable to CNP fraud victimization rather than cybercrime in general. The results of this study suggested that home users' online lifestyles affect the likelihood of becoming a victim of CNP fraud, which yielded support to the applicability of RAT to CNP fraud victimization.

These results provide significant implications for crime prevention efforts. First, the results suggested that online activities that require personal or financial information enhance the likelihood of experiencing CNP fraud victimization. This risk could be the outcome of either inadvertent contributions of home users or security breaches of online trading sites. In order to decrease criminal opportunities, individuals should be wary of providing their financial details over online communication platforms and online shopping sites. Additionally, online merchants may enhance their safeguarding measures to ensure safe transactions.

Second, being cautious about online purchasing via mobile phones may be another crime prevention measure. Mobile devices are mostly utilized at places where there are several distractors. Hence, the association between mobile phones/smartphones and increased risk of victimization may be attributed to the decreased attention while accessing the Internet via mobile devices. Impulsive buying may be another reason for this association. Home users who are using desktop/laptop computers at home may be making more sound decisions when compared to those who utilize mobile devices to purchase goods. Future research may also research this aspect of the study.

Lastly, the application of personal guardianship measures would be another efficient crime prevention and reduction method. Digital guardianship measures did not predict victimization, which suggests that CNP fraud victimization may be the outcome of non-technological interactions such as social engineering methods. Home users may prevent CNP fraud victimization by increased vigilance about their personal communications.

Acknowledgements

We would like to thank the UK Data Archive for providing the dataset of Crime Survey for England and Wales (CSEW) 2014/2015.

REFERENCES

Ahmad, Z., Zeki, A. M., & Olowolayemo, A. (2016). *Security Failures in EMV Smart Card Payment Systems.* Paper presented at the Information and Communication Technology for The Muslim World (ICT4M), 2016 6th International Conference on.

Akdemir, N. (2019). *Understanding the Individual Level and Macro Level Causes of Economic Cybercrime Victimisation in the UK: A Contextual Vulnerabilities Approach to Examine Cybercrime Victimisation.* Durham University.

Akdemir, N., Sungur, B., & Basaranel, B. U. (2020). Examining the Challenges of Policing Economic Cybercrime in the UK. *The Journal of Security Sciences Special Edition*, 111-132.

Anderson, R., & Murdoch, S. J. (2014). EMV: Why payment systems fail. *Communications of the ACM, 57*(6), 24-28.

Arango, C., Huynh, K. P., & Sabetti, L. (2015). Consumer payment choice: Merchant card acceptance versus pricing incentives. *Journal of Banking & Finance, 55*, 130-141.

Bossler, A. M., & Holt, T. J. (2009). Online Activities, Guardianship, and Malware Infection: An examination of Routine Activities Theory. *International Journal of Cyber Criminology*, *3*(1), 400.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*(3), 227-236.

Bouchard, M., Wang, W., & Beauregard, E. (2012). Social capital, opportunity, and school-based victimization. *Violence victims & Offenders, 27*(5), 656-673.

Branco, B., Abreu, P., Gomes, A. S., Almeida, M. S., Ascensão, J. T., & Bizarro, P. J. a. p. a. (2020). Interleaved Sequence RNNs for Fraud Detection.

Bulakh, V., & Gupta, M. (2015). *Characterizing credit card black markets on the web.* Paper presented at the Proceedings of the 24th International Conference on World Wide Web.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online Frauds: Learning from Victims why They Fall for These Scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391-408. doi:10.1177/0004865814521224

Ching, A. T., & Hayashi, F. (2010). Payment card rewards programs and consumer payment choice. *Journal of Banking & Finance, 34*(8), 1773-1787.

Choi, K.-s., Choo, K., & Sung, Y.-e. (2016). Demographic variables and risk factors in computer-crime: an empirical assessment. *Cluster Computing, 19*(1), 369-377.

Clarke, R. V. (1980). Situational crime prevention: Theory and practice. *Brit. J. Criminology, 20,* 136.

Clarke, R. V. (1995). Situational crime prevention. *Crime and justice*, 91-150.

Clarke, R. V., & Felson, M. (1998). *Opportunity makes the thief: Practical theory for crime prevention*. Retrieved from

Cohen, L. E., & Cantor, D. (1981). Residential burglary in the United States: Life-style and demographic factors associated with the probability of victimization. *Journal of Research in Crime and Delinquency, 18*(1), 113-127.

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

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory. *American Sociological Review, 46*(5), 505-524.

Corre, K., Barais, O., Sunyé, G., Frey, V., & Crom, J.-M. (2017). Why can't users choose their identity providers on the web? *Proceedings on Privacy Enhancing Technologies, 3,* 72-86.

Cross, C., Richards, K., & Smith, R. G. (2016). Improving responses to online fraud victims: An examination of reporting and support.

Dytham, C. (2011). *Choosing and using statistics: a biologist's guide*: John Wiley & Sons.

Field, A. (2009). *Discovering statistics using SPSS*: Sage publications.

Fisher, B. S., Daigle, L. E., & Cullen, F. T. (2010). What distinguishes single from recurrent sexual victims? The role of lifestyle-routine activities and first-incident characteristics. *Justice Quarterly, 27*(1), 102-129.

FTC. (2019). *Consumer Sentinel Network*. Retrieved from https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf

Garg, V., & Nilizadeh, S. (2013). *Craigslist scams and community composition: Investigating online fraud victimization.* Paper presented at the Security and Privacy Workshops (SPW), 2013 IEEE.

Gillespie, A. A., & Magor, S. (2020). *Tackling online fraud.* Paper presented at the ERA Forum.

Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? *Social and Legal Studies, 10*(2), 243-250.

Healey, J. F. (2014). *Statistics: A Tool for Social Research* (9 ed.). Belmont, CA: Wadsworth Publishing Company.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*: Ballinger Cambridge, MA.

Ho, R. (2013). *Handbook of univariate and multivariate data analysis with IBM SPSS*: CRC Press.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review, 31*(2), 165-177.

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

Holt, T. J., & Bossler, A. M. (2013). Examining the Relationship between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice*, 1043986213507401.

Holt, T. J., & Turner, M. G. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior, 33*(4), 308-323.

Holtfreter, K., Reisig, M., & Pratt, T. (2008). Low Self-Control, Routine Activities, and Fraud Victimization. *Criminology, 46*(1), 189-220.

Holtfreter, K., Reisig, M. D., Leeper Piquero, N., & Piquero, A. R. (2010). Low self-control and fraud: Offending, victimization, and their overlap. *Criminal Justice and Behavior, 37*(2), 188-203.

Howard, R. (2009). *Cyber fraud: tactics, techniques and procedures*: CRC press.

Hutchings, A., & Hayes, H. (2008). Routine activity theory and phishing victimisation: Who gets caught in the net. *Current Issues Crim. Just., 20*, 433.

Jackson, S. L. (2013). *Statistics plain and simple*: Cengage Learning.

Jansen, J., & Leukfeldt, R. (2015). *How people help fraudsters steal their money: An analysis of 600 online banking fraud cases.* Paper presented at the Socio-Technical Aspects in Security and Trust (STAST), 2015 Workshop on.

Jansen, J., & Van Schaik, P. J. C. i. H. B. (2018). Testing a model of precautionary online behaviour: The case of online banking. *87*, 371-383.

Jordan, G., Leskovar, R., & Marič, M. (2018). Impact of fear of identity theft and perceived risk on online purchase intention. *Organizacija, 51*(2), 146-155.

Kahn, C. M., & Liñares-Zegarra, J. M. (2016). Identity theft and consumer payment choice: Does security really matter? *Journal of Financial Services Research, 50*(1), 121-159.

Kennedy, L. W., & Forde, D. R. J. C. (1990). Routine activities and crime: An analysis of victimization in Canada. *28*(1), 137-152.

Kokh, M. T. (2019). Symantec Mobile Threat Defense: Using Mobile to Stay One Step Ahead of PC Attacks. Retrieved from https://symantec-blogs.broadcom.com/blogs/product-insights/symantec-mobile-threat-defense-using-mobile-stay-one-step-ahead-pc-attacks?es_p=10097396

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

Lipsman, A. (2019). Global Ecommerce 2019, Ecommerce Continues Strong Gains Amid Global Economic Uncertainty. Retrieved from https://www.emarketer.com/content/global-ecommerce-2019

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior, 31*(5), 381-410.

Meier, R. F., & Miethe, T. D. (1993). Understanding theories of criminal victimization. *Crime and justice,* 459-499.

Miethe, T. D., & McDowall, D. (1993). Contextual effects in models of criminal victimization. *Social Forces, 71*(3), 741-759.

Miethe, T. D., & Meier, R. F. (1990). Opportunity, choice, and criminal victimization: A test of a theoretical model. *Journal of Research in Crime and Delinquency, 27*(3), 243-266.

Miethe, T. D., & Meier, R. F. (1994). *Crime and its social context: Toward an integrated theory of offenders, victims, and situations*: Suny Press.

Miethe, T. D., Stafford, M. C., & Long, J. S. (1987). Social differentiation in criminal victimization: A test of routine activities/lifestyle theories. *American Sociological Review,* 184-194.

Mittal, S., & Tyagi, S. (2020). Computational Techniques for Real-Time Credit Card Fraud Detection *Handbook of Computer Networks and Cyber Security* (pp. 653-681): Springer.

Montague, D. A. (2010). *Essentials of online payment security and fraud prevention* (Vol. 54): John Wiley & Sons.

Mustaine, E. E., & Tewksbury, R. (1998). Predicting Risks of Larceny Theft Victimization: A Routine Activity Analysis Using Refined Lifestyle Measures. *Criminology, 36*(4), 829-858. doi:10.1111/j.1745-9125.1998.tb01267.x

Newman, G. R., & Clarke, R. V. (2013). *Superhighway robbery*: Routledge.

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

Office for National Statistics. (2020). *Crime Survey for England and Wales, 2014-2015*. [data collection]. *2nd Edition*. UK Data Service. SN: 7889, http://doi.org/10.5255/UKDA-SN-7889-2.

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice, 43*(4), 626-642.

Payton, M. E., Greenstone, M. H., & Schenker, N. (2003). Overlapping confidence intervals or standard error intervals: what do they mean in terms of statistical significance? *Journal of Insect Science, 3*(1), 34.

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

Rege, A. (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology*, *3*(2), 494-512.

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived Risk of Internet Theft Victimization. *Criminal Justice and Behavior, 36*(4), 369-384. doi:10.1177/0093854808329405

Reyns, B. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory Beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238. doi:10.1177/0022427811425539

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime*, *22*(4), 396-411.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International journal of offender therapy and comparative criminology*, *60*(10), 1119-1139.

Reyns, B. W., Henson, B., Fisher, B. S., Fox, K. A., & Nobles, M. R. (2016). A gendered lifestyle-routine activity approach to explaining stalking victimization in Canada. *Journal of Interpersonal Violence*, *31*(9), 1719-1743.

Sampson, R. J., & Wooldredge, J. D. (1987). Linking the micro-and macro-level dimensions of lifestyle-routine activity and opportunity models of predatory victimization. *Journal of Quantitative Criminology*, *3*(4), 371-393.

Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209-215.

See-To, E. W., Papagiannidis, S., & Westland, J. C. (2014). The moderating role of income on consumers' preferences and usage for online and offline payment methods. *Electronic Commerce Research*, *14*(2), 189-213.

Sendo, M. R., Sherman, R. S., & Kaltwasser, J. C. (2005). Methods and apparatus for conducting secure, online monetary transactions: Google Patents.

Shabir, G., Hamad, N., & Anosh, M. (2014). A True Picture of Electronic Business on Agriculture Sector of Southern Punjab, Pakistan. *International Journal of Innovative Research Development*, 2278-0211.

Singh, A., & Jain, A. (2020). A Novel Framework for Credit Card Fraud Prevention and Detection (CCFPD) Based on Three Layer Verification Strategy *Proceedings of ICETIT 2019* (pp. 935-948): Springer.

Smith, M., Bouffard, L. A. J. T. E. o. C., & Justice, C. (2014). Victim precipitation. 1-5.

Thomas, C., Thiry, J., Hsu, K., Traver, K., & Tengkiattrakul, P. (2014). Analysis of Online Credit Card Black Markets.

Turban, E., Outland, J., King, D., Lee, J. K., Liang, T.-P., & Turban, D. C. (2017). *Electronic commerce 2018: a managerial and social networks perspective*: Springer.

Van Wilsem, J. (2011). Worlds Tied Together? Online and Non-Domestic Routine Activities and Their Impact on Digital and Traditional Threat Victimization. *European Journal of Criminology, 8*(2), 115.

Van Wilsem, J. (2013a). Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization. *European Sociological Review, 29*(2), 168-178. doi:10.1093/esr/jcr053

Van Wilsem, J. (2013b). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437-453.

Vishal, V., & Johari, R. (2018). *SOAiCE: Simulation of Attacks in Cloud Computing Environment.* Paper presented at the 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence).

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4): Polity.

Wall, D. S. (2010). Micro-frauds: Virtual Robberies, Stings and Scams in the Information Age. In T. Holt & B. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 68-85): IGI Global.

Wolfgang, M. E. J. T. J. o. C. L., Criminology,, & Science, P. (1957). Victim precipitated criminal homicide. *48*(1), 1-11.

Yar, M. (2005). The Novelty of 'Cybercrime' an Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427.