Exploring the Human Factor in Cyber-enabled and Cyber-dependent Crime Victimisation: A Lifestyle Routine Activities Approach

Abstract

Purpose: The purpose of this study was to explore human factors as the possible facilitator of cyber-dependent (hacking and malware infection) and cyber-enabled (phishing) crimes victimisation, and to test the applicability of Lifestyle Routine Activities Theory (LRAT) to cybercrime victimisation.

Design/methodology/approach: A mixed methods research paradigm was applied to address the research questions and aims. The dataset of Crime Survey of England and Wales (CSEW) 2014/2015 and 42 semi-structured interviews conducted with victims of cybercrime and non-victim control group participants were analysed via binary logistic regression and content analyses methods.

Findings: This research illustrated that internet users facilitated their victimisation through their online activities. Additionally, using insecure internet connections and public access computers emerged as risk factors for both cyber-enabled and cyber-dependent crime victimisation. Voluntary and involuntary personal information disclosure through social networking sites and online advertisement websites increased the likelihood of being a target of phishing. Deviant online activities such as free streaming or peer-to-peer sharing emerged to increase the risk of cyber-dependent crime victimisation.

Research implications: The binary logistic regression analysis results suggested LRAT as a more suitable theoretical framework for cyber-dependent crime victimisation. Future research may test this result with models including more macro variables.

Practical implications: Policymakers may consider implementing regulations regarding limiting the type of information required to login to free Wi-Fi connections. Checking trust signs and green padlocks may be effective safeguarding measures to lessen the adverse impacts of impulsive buying.

Originality/value: This study empirically illustrated that, besides individual-level factors, macro-level factors such as electronic devices being utilised to access the internet and data breaches of large companies also increased the likelihood of becoming the victim of cyber-enabled and cyber-dependent crime.
1. Introduction

The internet can be utilised for a wide array of purposes, ranging from communication to trading. The integration of mobile technologies to the internet has also boosted the omnipresence of both in people’s lives (Holt and Bossler, 2016). It is estimated that approximately 89% of adults had internet access in the UK in 2018 (Office for National Statistics, 2018). The intrusion of the internet into every facet of life has not only provided new opportunities for the commission of traditional crimes (cyber-enabled and cyber-assisted crimes) in cyberspace, but has also given rise to the birth of new online crimes (cyber-dependent) (Grabosky, 2001; Wall, 2007).

Recent evidence suggests that cybercrime is on the rise (Levi, 2017). For example, 13,357 cybercrime cases were reported between April and September 2018, and victims of these cases lost £34.6 million in the UK (City of London Police, 2019). Human behaviour is perceived as the facilitator of victimisation. Research suggests that the human is the weakest chain in computer security (Evans et al., 2016), as human reasoning can be exploited by external manipulations (Cook and Fox, 2011). Likewise, Lifestyle Routine Activities Theory (LRAT) posits that individuals facilitate their victimisation through their routine activities and lifestyles (Cohen and Felson, 1979; Hindelang et al., 1978). Victim facilitation denotes victims’ inadvertent contributions to the occurrence of crime (Van Wyk and Benson, 1997). It may be perceived “as a catalyst in a chemical reaction that, given the right ingredients and conditions, speeds up the interaction” (Karmen, 2012, p. 124).

In summary, empirical studies testing LRAT’s propositions have illustrated the relationship between internet users’ online activities and the risk of experiencing cybercrime victimisation. The question that needs to be addressed is whether internet users’ online lifestyles pose the same risks for each category of cybercrime. The aim of this empirical research is to address this question and assess the applicability of LRAT to cyber-enabled
(phishing) and cyber-dependent (malware infection and hacking) crimes. Additionally, exploring the reasons for becoming a victim of cybercrime from victims’ perspectives was another goal of this research.

2. Theoretical Foundations

Lifestyle-Exposure Theory (LET), proposed by (Hindelang et al., 1978), was one of the first attempts to explain the causes of victimisation (Meier and Miethe, 1993). This theory sought to explain and understand violent victimisation across the demographic strata of the population. The central premise of LET is that individuals’ lifestyles increase the risk of being victimised by exposing them to potential offenders (Hindelang et al., 1978). Similarly, the Routine Activities Theory (RAT) of Cohen and Felson (1979) posits that individuals’ routine activities create opportunities for the commission of crime. According to these theories, crime occurs when a suitable target and a motivated offender converge in the absence of a guardian capable of deterring the threat (Cohen and Felson, 1979). Later, Hindelang et al. (1978) and Miethe and Meier (1990) merged elements of LET and RAT into one single theory (LRAT). Although LRAT was proposed to explain traditional crimes, this approach has been extensively applied to cybercrime research (Vakhitova et al., 2015).

LRAT is an opportunity-based crime theory that focuses on criminal opportunities created by individuals’ daily routine activities (Miethe and Meier, 1990). It is argued that people’s actions, which enhance their exposure to would-be offenders, contribute to the chances of becoming a target (Miethe and McDowall, 1993). Hindelang et al. (1978, p. 61) argue that variations in lifestyles impact the risk of exposure to offenders at specific times and places, since “victimisation is not randomly distributed across time and space”. The more time spent outside home settings, the more likely individuals are to face victimisation, due to an increased chance of interacting with offenders in precarious places and at risky times (Mustaine and Tewksbury, 2000). Further, the attractiveness of potential targets and the degree of capable
guardianship impact offenders’ target selection decisions, given that offenders act rationally (Miethe and Meier, 1990). Exposure/proximity to the motivated offender, target suitability and absence of guardianship are three core concepts of LRAT.

**Exposure/Proximity to Motivated Offenders:** Exposure to offenders, which denotes “the physical visibility and accessibility of persons or objects to potential offenders” (Cohen et al., 1981, p. 507), is one of the central elements of LRAT. LRAT perceives individuals’ leisure and vocational activities as the facilitators of crime (Eck, 1995). Past traditional crime studies found that activities outside the home setting enhanced the exposure/proximity to motivated offenders, thereby increasing the risk of victimisation (Tillyer et al., 2011). Similarly, cybercrime victimisation studies have suggested that exposure/proximity to online perpetrators increased the likelihood of victimisation (Holt and Bossler, 2013; Jansen and Leukfeldt, 2015).

**Target Suitability:** Target suitability refers to being vulnerable or open to perpetrators’ actions (Finkelhor and Asdigan, 1996). Target suitability has two dimensions: routine activities that make individuals or objects suitable targets, and attributes of individuals or objects that make them attractive targets (Cohen et al., 1981). Previous cybercrime studies examined the relationships between demographic characteristics such as income, age and gender and the risk of victimisation (Dai et al., 2014; Policastro and Payne, 2014). However, the relationship between the digital components of cyberspace, namely electronic devices utilised to access the internet, and cybercrime victimisation is under-researched. This study addresses this gap by operationalising electronic devices as target suitability components of the LRAT victimisation model.

**Absence of Capable Guardianship:** LRAT proposes that the absence of a guardian capable of deterring a threat increases the chances of experiencing crime victimisation. A capable guardian is not only perceived as a means of impeding an immediate threat, but is also a factor alleviating target attractiveness (Cohen et al., 1981). Traditional crime studies categorised
guardianship measures as physical (e.g. alarms, fences) and social (e.g. presence of family members) (Miethe and Meier, 1990). Cybercrime studies grouped guardianship measures as digital (e.g. anti-virus programs or firewalls) and personal (e.g. using complex passwords). Cyber-interpersonal victimisation (e.g. cyberbullying, online harassment) studies include social guardianship (such as the presence of a teacher or family member) as a third type of guardianship measure. The results of previous cybercrime studies yielded mixed results concerning the effectiveness of guardianship measures in preventing cybercrime. Whereas the results of some studies suggested that guardianship measures decreased the risk of victimisation (Williams, 2015), the results of others indicated that the application of online security measures increased the risk of victimisation (Ngo and Paternoster, 2011; Reyns et al., 2016). These studies suggested the cross-sectional nature of the research design as the possible explanation for the increased risk posed by the application of guardianship measures. Some other cybercrime studies found no association between guardianship measures and cybercrime victimisation (Leukfeldt, 2014; van Wilsem, 2013b).

3. Literature Review

Providing a typology of cybercrime is a contested issue in the cybercrime literature. Several scholars (Brenner, 2010; Gordon and Ford, 2006; Higgins and Wolfe, 2009; Wall, 2007) and institutions (e.g. Council of Europe) [1] have provided typologies of cybercrime (Table 1), using varying criteria to classify cybercrime into categories. Whereas Higgins and Wolfe (2009) focused on the opportunities that each category of cybercrime created for different offending groups, Gordon and Ford (2006) perceived cybercrime as a continuum with technology-based crimes at one end and people-based crimes at the other. Brenner (2010) classified cybercrime from a law perspective. On the other hand, Wall (2007) utilised the role
of Information and Communications Technology in the commission of crime, while categorising cybercrimes as cyber-enabled, cyber-dependent and cyber-related.

Though Wall’s classification is criticised for focusing solely on the means of attack and neglecting intended outcomes and motivations (Furnell et al., 2015), it is the most widely accepted and utilised typology (Bergmann et al., 2018; Levi et al., 2015; McGuire and Dowling, 2013). Cyber-dependent crimes, also labelled as true cybercrimes, are offences that can only be committed via networked internet technologies; this genre of crime vanishes when networked internet technologies are removed from the equation (Wall, 2010). Malware infection, hacking and spamming are the most vivid examples of this new genre of cybercrime (McGuire and Dowling, 2013). Cyber-enabled crimes are hybrid cybercrimes, which are the outcome of the integration of traditional crimes and networked technologies (Wall, 2007). Networked technologies have become an environment for the commission of this type of crime (Wall, 2010). The crime persists after the removal of networked technologies, but most of the opportunities, such as the opportunity to conduct large-scale attacks or access individuals living in remote locations, would be lost (Levi et al., 2015). Phishing (the fraudulent practice of sending emails purporting to be from legitimate sources for the purpose of extracting information such as credit-card details), large-scale fraud, identity theft and online pornography are examples of this.

3.1 Determinants of Becoming a Victim of Cybercrime

Cyber-enabled Crimes

Extant cybercrime research on phishing has mainly focused on discerning the factors that render individuals susceptible to socially engineered email messages (i.e. Jansen and Leukfeldt, 2015; Silic and Back, 2016; Williams and Levi, 2017; Wright et al., 2014). Only a
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title 1  Offences against the confidentiality, integrity and availability of computer data and systems</td>
<td>Cyber-dependent Crimes (Crimes against the machines) *Malware Infection *Cyber-trespass *Hacking/Cracking</td>
<td>Target cybercrimes *Hacking *Malware infection</td>
<td>Cyber community *Hacking *Cracking</td>
<td>Type I Cybercrime *Phishing *Hacking *Identity Theft</td>
</tr>
<tr>
<td>Title 2  Computer-related offences</td>
<td>Cyber-enabled Crimes (Crimes using the machines) *Cyber-deceptions *Fraud</td>
<td>Tool cybercrimes *Fraud</td>
<td>Cyber fraud</td>
<td>Type II Cybercrime *Cyberstalking *Extortion *Blackmail</td>
</tr>
<tr>
<td>Title 3  Content-related offences *Child Pornography</td>
<td>Content-related offenses (Crimes in the machines) Cyber-obscenity Cyber-violence/harm</td>
<td>Computer incidental *Real world crimes using computers</td>
<td>Cybermarkets *Digital piracy *Cyberpornography</td>
<td></td>
</tr>
<tr>
<td>Title 4  Offences related to infringements of copyright and related rights</td>
<td>*Digital piracy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
handful of studies (Jansen and Leukfeldt, 2016; Leukfeldt, 2014; Reynolds, 2015) have examined the behavioural determinants of becoming a phishing target or victim from an LRAT perspective. Studies conducted by Ngo and Paternoster (2011), Paek and Nalla (2015) and Reynolds (2015) suggested that legitimate online activities, such as shopping, booking, banking and social networking, increase the odds of becoming a phishing target. Posting personal information online also emerged as a strong predictor of becoming a target of phishing (Halevi et al., 2013; Seng et al., 2018). However, the results of Jansen and Leukfeldt (2016) and Leukfeldt (2014) suggested no association between online activities and the odds of becoming a phishing victim.

**Cyber-dependent Crimes**

Malware covers a wide range of code-based online threats such as computer viruses, Trojan horses or keyloggers. Infected files, freely distributed programs or websites are utilised to infect target electronic devices (Ma et al., 2012). Malware infection poses a significant threat to electronic devices’ security as well as internet users’ personal information and privacy (Bettany and Halsey, 2017). According to Symantec’s recent internet security report, one in every 3,207 emails contained malware. Moreover, in 2018, 7.8% of emails contained malicious URLs used to divert internet users onto bogus websites (Symantec, 2019).

Previous research examining the relationship between legitimate online activities and the risk of malware infection reported conflicting results. On one hand, legitimate online activities such as shopping, social networking, booking (Reyns, 2015), downloading, gaming (Leukfeldt, 2015), movies, dating websites (Holt et al., 2018), and accessing the internet frequently (Bergmann et al., 2018) were found to be associated with the risk of malware infection. On the other hand, engaging with online deviant activities was also identified as a
risk factor for infection (Holt and Bossler, 2013). For instance, the results of Holt and Bossler
(2013), who examined the relationship between routine online activities and malware infection,
showed that the risk of malware infection increased by engaging with deviant rather than
legitimate online activities. They identified viewing pornography, unauthorised access to
someone’s internet connection and pirating media as the correlates of malware infection.

Hacking is the unauthorised access to computers or computer systems with the aim of
damaging, altering or stealing data (Wall, 2001). Hackers utilise technical subterfuge such as
malware infection or social engineering to access computer systems (Hutchings, 2013; Reyns
and Henson, 2016). Although the initial hackers were motivated by naïve ends, such as
curiosity or identifying deficiencies in computer systems, recent hackers have been motivated
more by criminal intent, such as financial gain or terrorism (Koops, 2010). Wall (2015)
explained this shift in the hacker stereotype with the increased commercialisation of the internet
and the myriad opportunities arising from this.

Cybercrime victimisation studies (Holt and Copes, 2010; Leukfeldt and Yar, 2016;
Reyns, 2015) have researched the antecedents of becoming a hacking victim. The results of
these studies suggested participating in online forums, sharing personal information on social
media, pirating media, and accessing adult content as risk factors for hacking victimisation.
Additionally, the relationships between hacking and online harassment (van Wilsem, 2013b),
identity theft (Reyns and Henson, 2016) and malware infection (Chu et al., 2010) have been
researched. The results of these studies indicate a mutual relationship between hacking
victimisation and these forms of cybercrime victimisation.

In this research, prior cybercrime victimisation research has been extended in four
aspects.
First, previous cybercrime studies testing the applicability of LRAT to cybercrime either examined its applicability to a specific type of cybercrime (i.e., hacking or phishing), or to all types of cybercrime victimisation. This research was one of the first empirical attempts to assess the applicability of LRAT to specific categories of cybercrime, such as cyber-enabled and cyber-dependent crime. This approach enabled us to examine the role of human factors in the occurrence of cybercrime victimisation, and to consider with greater precision the relationship between these human factors and specific categories.

Second, previous cybercrime studies mainly focused on the impact of individual-level factors on the risk of victimisation. This study incorporates aggregate level elements into the cybercrime victimisation model. Holt et al. (2018) demonstrated that having a secure wireless connection lessened the risk of malware infection. This result proposes that the type of internet connection may affect the likelihood of becoming a cybercrime victim. This study included electronic devices used away from secure internet connections as the target suitability element of LRAT. This is the first empirical study examining the impact of high-risk mobile electronic devices on the likelihood of experiencing cybercrime victimisation.

Third, previous studies researching the correlates of cybercrime victimisation were mostly quantitatively driven (Choi et al., 2016; Reyns et al., 2016; van Wilsem, 2011), with only a few qualitative studies in existence (Burgard and Schlembach, 2013; Jansen and Leukfeldt, 2016). This study is one of the first cybercrime victimisation studies in which a mixed methods research paradigm has been applied to understand the causes of cybercrime victimisation through opportunity theories. A mixed methods research design, where qualitative and quantitative research approaches are combined to achieve “breadth and depth of understanding and corroboration” (Johnson et al., 2007, p. 123), provided some useful insights. This enabled us to address the pitfalls of survey data. For example, online deviance was not measured in the survey. Qualitative data addressed this shortcoming of the secondary
data. Qualitative data also provided new insights, such as the impact of data breaches of large companies on the risk of becoming a target of phishing. This will be addressed in the Discussion section.

Lastly, many cybercrime studies utilised college students as a sample universe (e.g. Holt and Bossler, 2013; Ngo and Paternoster, 2011). However, the generalisability of research results based on such a sample universe is questionable, since the internet skills of college students are expected to be better than those of older generations (van Wilsem, 2013b). Such studies moreover are unlikely to capture fully an appropriate demographic balance. This study addresses this gap by utilising a national sample of England and Wales, and by also selecting respondents for qualitative research on the basis of age and income.

4. Hypotheses

4.1 Exposure/Proximity to Motivated Offender

Cybercrime studies researching the impact of normal or legitimate online activities on the risk of victimisation illustrated that internet users expose their personal and financial information willingly or inadvertently to perpetrators through their online actions (Holt et al., 2018; Leukfeldt and Holt, 2019). Shopping (Marcum et al., 2010; Pratt et al., 2010; Reyns, 2013), banking (Leukfeldt and Yar, 2016; Reyns, 2015) and social activities (i.e. using chatrooms, visiting internet forums) (Tonellotto, 2020; van Wilsem, 2013b) thus far have been linked with increased exposure to online perpetrators, thereby enhancing the likelihood of becoming a victim of cybercrime. Hence, it was hypothesised that:

\[ H1a: \text{Legitimate online activities increase exposure/proximity to motivated offenders, thereby enhancing the risk of cybercrime victimisation.} \]

Besides legitimate activities, a number of empirical studies reported deviant online activities as a risk factor for cybercrime victimisation. Deviant or illegal behaviours include
viewing or downloading pornography (Ngo and Paternoster, 2011), pirating and sharing pirated media (David, 2017; Ngo and Paternoster, 2011), hacking (Donner et al., 2014; Ngo and Paternoster, 2011), free streaming (Kirton and David, 2013; Wong, 2016) and downloading software illegally (Donner et al., 2014; Paek and Nalla, 2015).

The results of these studies suggested an association between deviant activities and the risk of experiencing cybercrime victimisation. For instance, recent evidence suggests accessing adult content or engaging with digital piracy as a significant antecedent of becoming a victim of malware infection (Holt and Bossler, 2013). Opening unknown email attachments or downloading free games was found to be associated with an increased risk of online identity theft victimisation (Ngo and Paternoster, 2011; Reyns, 2013). Past research examining the technical modus operandi of online perpetrators established the relationship between free streaming websites and malware infection. For instance, Rafique et al. (2016) examined free live streaming domains to investigate the risk posed by these sorts of websites. Their study illustrated that users of these websites were exposed to malware and malicious browser extensions. Similarly, Hsiao and Ayers (2019), who compared legitimate and illegal live streaming services' behaviours, found that users who accessed illegal live streaming websites pose a risk of malware infection. Hence, the study hypothesised that:

\[ H1b: \text{ Engaging with deviant online activities increases exposure/proximity to motivated offenders and thereby enhances the risk of cybercrime victimisation. } \]

4.2 Target Attractiveness

Cyberspace is a digital environment consisting of three layers, namely physical, logical and social, and five components, geographical, logical network, physical network, persona, and cyber-persona (Pamphlet, 2010). Electronic devices used to access the internet are part of the physical network components of the physical layer. It is a well-established fact that every
device bears some security risks that could be exploited by online perpetrators (Landman, 2010). Electronic devices such as laptops used away from secure internet connections are vulnerable to external threats (Watts, 2016), since fraudsters sometimes offer free Wi-Fi connections or interfere with legitimate Wi-Fi connections to steal the personal information of individuals at airports or shopping malls (Straw, 2013). Thus, it is hypothesised that:

**H2a: Connecting to the Internet through electronic devices utilising insecure connections increases target suitability, which in turn enhances the odds of becoming a victim of cyber-dependent and cyber-enabled crime.**

Additionally, public computers (e.g. in a library or internet café) may sometimes be used to access the internet. This could be considered as a risk factor, as these computers may not be monitored effectively. Zimerman (2010) illustrated how public computers in libraries were vulnerable to malware infection. Hutchings (2014) indicated that offenders utilise public access computers to conduct cyberattacks, which in turn infects these devices with malicious content. Williams (2015) suggested that individuals who frequently access the internet through public access computers were at increased risk of online identity theft. Thus, it was hypothesised that:

**H2b: Public access computers increase the risk of becoming a victim of cyber-enabled and cyber-dependent crime.**

### 4.3 Absence of Capable Guardianship

LRAT postulates that crime occurs in the absence of capable guardianship. Previous cybercrime research suggested that digital guardianship measures (i.e. anti-virus software) did not have a significant impact on the risk of victimisation (Leukfeldt, 2014; van Wilsem, 2013b). Yet, personal guardianship measures (i.e. presence of a teacher or parent) were reported as capable guardianship (Marcum et al., 2010; Williams, 2015). These studies however utilised
small samples to test the central postulates of LRAT. This study used a wider and more nationally representative sample, to hypothesise that:

\[ H3: \text{Online guardianship measures decrease the likelihood of becoming a victim of cyber-dependent and cyber-enabled crime victimisation.} \]

5. Method

5.1 Data

This study utilised the Crime Survey of England and Wales (CSEW) 2014/2015 (Office for National Statistics, 2016a), and semi-structured interviews conducted with victims of cybercrime and non-victim control group participants, to address the research question: “What are the risks posed by individuals’ online lifestyles for cyber-dependent and cyber-enabled crimes?” The CSEW, previously the British Crime Survey, has measured the nature and extent of crime in England and Wales since 1982 (Kantar Public, 2015). It was conducted with two year intervals until 2001, and since then it has been carried out annually (Jansson, 2007). The main aim of this survey is to observe trends and examine the risk factors for each type of crime in England and Wales. The CSEW 2014/2015 interviewed 35,000 adults aged over 16 (Office for National Statistics, 2016b).

A total of 32 semi-structured interviews with victims of cybercrime and ten semi-structured interviews with non-victim control group participants were conducted. The sampling process was informed by a maximum variation purposive sampling strategy. Internet users who had experienced financial loss over the internet in the last 12 months were recruited between December 2016 and November 2017. The control group included participants who had accessed the internet in the last 12 months but had not experienced cybercrime victimisation. Since the results of previous cybercrime studies indicated the impact of demographic characteristics on the risk of becoming a victim of cybercrime (Choi et al., 2016; Paek and
Nalla, 2015; van Wilsem, 2013a), a quota sampling strategy was adapted to obtain a demographically balanced sample.

The study was conducted according to the ethical principles of the Declaration of Helsinki (World Medical Association, 2001). Durham University School of Applied Social Sciences Ethics Committee approval was obtained in October 2016. Interviewees were asked to read the participant information sheet prior to the interviews. Participants were also provided with information related to protecting their identity, given the opportunity to abstain from responding to any unwanted questions, and to quit the interview process at any time before signing the consent form.

Audio-recorded interviews were transcribed verbatim, and voice files were deleted immediately after the transcription process. Participants were asked to detail the occurrence of victimisation. Whereas some participants reported losing money as a result of responding to unsolicited emails or providing financial information to bogus websites (phishing), some others acknowledged financial loss after experiencing unauthorised access to their online banking accounts or other online financial accounts (hacking). Additionally, some respondents reported unwanted alerts such as notifications from police forces about accessing illegal content (malware infection). Based on the participants’ accounts, the participants were classified into four distinct groups: phishing victims (14), hacking victims (ten), victims of multiple incidents (five), and victims of malware infection (three).

5.2 Measures

Dependent Variables:

Cyber-dependent crime (hacking and malware infection) and cyber-enabled crime (phishing) victimisation were dependent variables for the quantitative analysis of this study. To identify victims of cybercrime, the CSEW 2014/2015 asked respondents whether they had
experienced: unauthorised access to or use of personal data (hacking victimisation), a computer virus or other computer infection (malware infection), or loss of money through responding to communication (phishing). All of these measures were coded as dichotomous variables (0 = No, 1 = Yes).

Independent Variables:

**Exposure and proximity to motivated offenders**: LRAT proposes that individuals’ lifestyles, which increase exposure and proximity to motivated offenders, enhance the chances of being a victim of a crime. Seven online activities were included in the analysis: (1) banking or managing finances; (2) buying goods or services; (3) government services; (4) social networking; (5) email, instant messaging, chat rooms; (6) browsing for news or information; and (7) playing games/doing quizzes/competitions. All of the variables were dichotomised (0 = No, 1 = Yes).

**Target Suitability**: It was hypothesised that electronic devices bearing technological vulnerabilities might render internet users as suitable targets for online perpetrators. Two electronic devices, (1) laptop used away from home/work/school/college, and (2) public access computers, were operationalised as high-risk electronic devices due to inherent technological vulnerabilities.

**Absence of Capable Guardianship**: LRAT posits that capable guardianship may prevent the occurrence of victimisation. A total of 14 guardianship measures were included in the analyses to assess the impact of safeguarding measures on the risk of experiencing victimisation. However, irrelevant guardianship measures were excluded from the binary logistic regression models. For instance, the guardianship measure of logging out of websites when finished may be a capable measure for hacking victimisation, but it may not prevent phishing victimisation or malware infection. Hence, this guardianship measure was only
included in the hacking victimisation model while conducting the analysis. Guardianship
measures included in the analysis are as follows: (1) only downloading known files or
programs; (2) downloading software updates and patches whenever prompted; (3) using
complex passwords (containing letters, numbers and symbols); (4) using different passwords
for each different online account; (5) deleting suspicious emails without opening them; (6)
logging out of websites when finished; (7) adjusting website account settings (e.g. privacy
settings); (8) installing anti-virus or other security software, such as a firewall; (9) scanning
computers regularly for viruses or other malicious software; (10) protecting home Wi-Fi with
a password or being cautious using public Wi-Fi; (11) only using well-known or trusted sites;
(12) checking for signs that a site is secure before buying online; (13) only adding known
persons as friends on social networks; and (14) being careful about putting personal details on
social networking sites. All of the variables were dichotomously coded (0 = No, 1 = Yes).

6. Analytic Strategy

This study applied a sequential mixed methods strategy to examine the impacts of
individuals’ online lifestyles on the risk of facing cyber-dependent and cyber-enabled crime
victimisation. Bivariate and multivariate statistical analyses of CSEW 2014/2015 were
conducted prior to conducting the interviews. The interview guide was formed according to the
initial results of the quantitative phase of the study. Hence, the second part of the study
addressed the weakness of the survey dataset as well as enabling me to extend and understand
the results obtained in the initial phase.

Initially, bivariate analyses were conducted to observe the relationship between LRAT
constructs and cybercrime victimisation. Although some prior studies (Pratt et al., 2010;
Reyns, 2013) preferred using Pearson’s correlation test while examining the relationship
between categorical variables, it is suggested that Pearson’s Chi-square test is more appropriate
to explore the associations between two categorical variables (Blaikie, 2003), since Pearson’s
correlation measures the linear associations. Hence, Pearson’s Chi-square tests were conducted to examine the bivariate associations between cybercrime victimisation and independent variables.

The aim in the second qualitative phase of the analysis was to understand the underlying reasons for becoming a victim of cybercrime, and extend the results obtained in the first quantitative stage. To these ends, a conventional content analysis method was employed to obtain a systematically analysed, replicable and valid account of cybercrime victimisation through the victims’ own experiences (Hsieh and Shannon, 2005). The three-staged (data reduction, data display, and conclusion drawing/verification) interactive model of qualitative data analysis of Miles and Huberman (1994) was utilised while analysing the interview transcripts with the help of QSR NVivo software. This analysis started with coding the textual data. Codes demonstrating similarities were grouped under parent categories. Later, these interrelated categories were grouped to discern the themes (Saldaña, 2015). Later, these emergent themes were juxtaposed to the results of the initial quantitative phase to derive meaningful interpretations of the research findings.

7. Results

7.1 Quantitative Analysis Results

Bivariate Associations

As shown in Table 2, approximately all variables related to exposure and proximity to motivated offenders were significantly associated with malware infection and hacking. However, the Phi coefficient test values ranging from 0.003 to 0.131 suggest that all of the relationships were weak.

Bivariate associations between online guardianship measures and cybercrime victimisation were also examined. The bivariate analysis results displayed in Table 3 illustrate
Table 2

<table>
<thead>
<tr>
<th>Exposure and Proximity to Motivated Offenders</th>
<th>Malware Infection</th>
<th></th>
<th>Hacking</th>
<th></th>
<th>Phishing</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$Ph$</td>
<td>Chi-square Tests</td>
<td>$Ph$</td>
<td>Chi-square Tests</td>
<td>$Ph$</td>
<td>Chi-square Tests</td>
</tr>
<tr>
<td>Online banking or managing finances (e.g. paying credit cards)</td>
<td>0.0</td>
<td>51.318**</td>
<td>0.0</td>
<td>24.733**</td>
<td>0.0</td>
<td>4.882*</td>
</tr>
<tr>
<td>Buying goods or services (e.g. Internet shopping, music / film downloads)</td>
<td>95</td>
<td>*</td>
<td>66</td>
<td>*</td>
<td>29</td>
<td>5.912*</td>
</tr>
<tr>
<td>Online government services (e.g. tax returns, council tax, benefits)</td>
<td>0.0</td>
<td>51.080**</td>
<td>0.0</td>
<td>34.002**</td>
<td>0.0</td>
<td>4.882*</td>
</tr>
<tr>
<td>Social networking (e.g. Facebook, Twitter) or blogging</td>
<td>95</td>
<td>*</td>
<td>77</td>
<td>*</td>
<td>32</td>
<td>2.647</td>
</tr>
<tr>
<td>E-mail, instant messaging, chat rooms</td>
<td>0.1</td>
<td>74.612**</td>
<td>0.0</td>
<td>33.928**</td>
<td>0.0</td>
<td>17.073**</td>
</tr>
<tr>
<td>Browsing for news or information (e.g. BBC, Wikipedia)</td>
<td>15</td>
<td>*</td>
<td>77</td>
<td>*</td>
<td>55</td>
<td>*</td>
</tr>
<tr>
<td>Playing online games/doing quizzes/competitions</td>
<td>0.0</td>
<td>50.421**</td>
<td>0.0</td>
<td>10.042**</td>
<td>0.0</td>
<td>0.037</td>
</tr>
<tr>
<td>Laptop (away from home and work or school/college)</td>
<td>94</td>
<td>*</td>
<td>42</td>
<td>*</td>
<td>03</td>
<td>0.070</td>
</tr>
<tr>
<td>Public access computer (e.g. in a library, internet cafe)</td>
<td>0.0</td>
<td>15.680**</td>
<td>0.0</td>
<td>4.319</td>
<td>0.0</td>
<td>0.700</td>
</tr>
</tbody>
</table>

*=p ≤0.05 **=p ≤0.01 ***=p ≤0.001
<table>
<thead>
<tr>
<th>Online Guardianship</th>
<th>Malware Infection</th>
<th>Hacking</th>
<th>Phishing</th>
</tr>
</thead>
</table>
|                                                        | Ph \(i\)          | Chi-
|                                                        | square Tests     | Ph \(i\)          | Chi-
|                                                        |                   | square Tests     | Tests |
| Only downloading known files or programs                | 0.06              | 21.609  | 0.04    | 8.884*  | 0.00  | 0.001 |
| Downloading software updates and patches whenever        | 0.00              | 12.274  | 0.00    | 18.744  | 0.05  | 0.139 |
| Using complex passwords (contain letters, numbers, and symbols) | 0.11              | 69.411  | 0.08    | 38.602  | 0.02  | 4.672* |
| Using a different password for each different online account | 0.02              | 3.605   | 0.02    | 25.231  | 0.00  | 0.029 |
| Deleting suspicious emails without opening them         |                   |         |         |         |       |
| Logging out of websites when you are finished           |                   |         |         |         |       |
| Adjusting website account settings (e.g. privacy settings) | 0.18              | 190.87  | 0.06    | 22.343  | 0.03  | 5.235* |
| Installing anti-virus or other security software, such as a firewall | 0.00              | 0.00    | 0.00    | 0.00    | 0.00  | 0.00  |
| Scanning computer regularly for viruses or other malicious software | 0.18              | 188.50  | 0.04    | 10.825  | 0.01  | 0.769 |
| Protecting your home wireless connection (Wi-Fi) with a password or been cautious using public Wi-Fi | 0.00              | 0.00    | 0.00    | 0.00    | 0.00  | 0.00  |
| Only using well-known or trusted sites                  |                   |         |         |         |       |
| Checking for signs that a site is secure before buying online | 0.00              | 0.00    | 0.00    | 0.00    | 0.00  | 0.359 |
| Only adding known persons as friend on social networks  |                   |         |         |         |       |
| Been careful about putting personal details on social networking sites | 0.00              | 0.00    | 0.00    | 0.00    | 0.00  | 0.309 |

*=p \leq 0.05 \quad **=p \leq 0.01 \quad ***=p \leq 0.001
that most of the online guardianship measures were significantly associated with malware infection and hacking. While the strength of associations between online guardianship measures and malware infection was moderate, those between hacking, phishing and online guardianship measures were weak.

**Multivariate Analysis**

All of the assumptions of binary logistic regression were checked prior to conducting the multivariate analyses. The absence of multicollinearity among independent variables is the most essential assumption of binary logistic regression analysis (Field, 2009). Variance Inflation Factor (VIF) was utilised to diagnose the presence of multicollinearity, which signifies a high intercorrelation among independent variables, prior to running the multivariate statistical tests, since the existence of multicollinearity may lead to unreliable predictions. VIF values ranging from 1.001 to 1.276 suggested the absence of multicollinearity among independent variables. All other assumptions, such as the dependent variable being a binary coded variable, and independence of observations, were also satisfied.

**Malware Infection:** Binary logistic regression analysis results indicate that when holding other variables constant, accessing the internet for online government services and email/instant messaging/chat rooms significantly predicted malware infection, providing support to H1a (Table 4). Whereas users who accessed the internet for online government websites were 29% (Exp. (B) = 1.288) more likely to be victims of malware infection, those who accessed the internet for email/instant messaging/chat rooms were 47% more likely to be victimised (Exp. (B) = 1.473) when compared to those who did not access the internet for those purposes. These results are in line with previous research demonstrating the association
between legitimate online activities and the risk of malware infection (Holt et al., 2018; Leukfeldt, 2015; Reyns, 2015).

The use of high-risk devices (laptops used away from home/work/school/college and public access computers) appeared to increase the risk of malware infection. Public access computers seemed to pose higher risks. Those who accessed the internet at public places were 1.6 times (Exp. (B) = 1.638) more likely to be a victim of malware infection. These results support H2a and H2b, suggesting a relationship between the risk of victimisation and accessing the internet through insecure connections and at insecure locations.

Three online guardianship measures emerged to be significant predictors of malware infection. The directions of the relationship were somewhat contrary to expectations. Installing anti-virus or other security software (Exp. (B) = 2.062) and scanning computers regularly for viruses or other malicious software (Exp. (B) = 1.599) appeared to increase the risk of victimisation. Only downloading known files or programs seemed to decrease the risk of victimisation. Users who only downloaded known files or programs were approximately 21% less likely to be a victim of malware infection (Exp. (B) = 0.791). These results yielded partial support for H3, stating that guardianship measures would decrease the risk of victimisation. The Cox & Snell R Square value of the model was 0.064, which means that the binary logistic regression model explained 6% of the variations.

**Hacking Victimisation:** The second binary logistic regression model suggested buying goods or services and email/instant messaging/chat rooms as significant predictors of hacking victimisation (Table 4). Users who accessed the internet mostly for buying goods or services were 82% more likely to be victims of hacking (Exp. (B) = 1.823). Likewise, users who accessed the internet for email/instant messaging/chat rooms were approximately 139% more likely to be victimised (Exp. (B) = 2.397), thereby providing support for H1a. These results
support previous studies (Leukfeldt and Yar, 2016; Reyns, 2015), suggesting an association between online activities and an increased risk of experiencing hacking victimisation.

Accessing the internet through a public access computer increased the risk of victimisation by 66% (Exp. (B) = 1.666), providing support for H2b. Online safeguarding measures, such as using different passwords for different accounts, deleting suspicious emails, logging out of websites when finished and installing anti-virus software or other security software, emerged to be significant predictors of hacking victimisation. However, nearly all of these online guardianship measures appeared to increase the risk of becoming a hacking victim (Exp. (B) = 1.302; 1.77; 0.718 and 1.381 respectively). These results contradict H3 proposing a negative relationship between the risk of victimisation and guardianship measures. The Cox & Snell R Square value of the binary logistic regression model was 0.021. This means that only 2.1% of the variations were explained by the model.

**Phishing Victimisation:** None of the online lifestyle variables and guardianship measures significantly predicted phishing victimisation (Table 4). This result accords with prior research suggesting a lack of association between online activities and the risk of victimisation (Leukfeldt, 2014), and contradicts (Reyns, 2015), whose results indicated a relationship between increased risk of phishing victimisation and online activities such as banking, shopping and social networking. This contradicts H1a, stating that engaging with legitimate online activities increases the likelihood of becoming a victim of cybercrime.

Accessing the internet via public access computers increased the risk of phishing victimisation by approximately 123% (Exp. (B) = 2.234), yielding support for H2b. The Cox & Snell R Square value of the binary logistic regression model was 0.004, indicates that the model explained only 0.4% of the variances.
Table 4

**Binary Logistic Regression Analysis**

<table>
<thead>
<tr>
<th>Variables in the Equation</th>
<th>Malware Infection</th>
<th>Hacking</th>
<th>Phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exp(B)</td>
<td>Exp(B)</td>
<td>Exp(B)</td>
</tr>
<tr>
<td>Exposure and Proximity to Motivated Offenders</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online banking or managing finances (e.g. paying credit cards)</td>
<td>1.043</td>
<td>1.094</td>
<td>1.191</td>
</tr>
<tr>
<td>Buying goods or services (e.g. Internet shopping, music/film downloads)</td>
<td>0.970</td>
<td>1.823*</td>
<td>1.549</td>
</tr>
<tr>
<td>Online government services (e.g. tax returns, council tax, benefits)</td>
<td>1.288**</td>
<td>1.182</td>
<td></td>
</tr>
<tr>
<td>Social networking (e.g. Facebook, Twitter) or blogging</td>
<td>0.950</td>
<td>1.173</td>
<td>1.234</td>
</tr>
<tr>
<td>E-mail, instant messaging, chat rooms</td>
<td>1.473**</td>
<td>2.397**</td>
<td></td>
</tr>
<tr>
<td>Browsing for news or information (e.g. BBC, Wikipedia)</td>
<td>1.187</td>
<td>0.881</td>
<td></td>
</tr>
<tr>
<td>Playing online games/doing quizzes/competitions</td>
<td>1.082</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Suitability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Laptop (away from home and work or school/college)</td>
<td>1.294***</td>
<td>1.163</td>
<td>1.121</td>
</tr>
<tr>
<td>Public access computer (e.g. In a library, internet cafe)</td>
<td>1.638***</td>
<td>1.666**</td>
<td>2.234**</td>
</tr>
<tr>
<td>Online Guardianship</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Only downloading known files or programs</td>
<td>0.791**</td>
<td>0.901</td>
<td></td>
</tr>
<tr>
<td>Downloading software updates and patches whenever prompted</td>
<td>0.973</td>
<td>0.932</td>
<td></td>
</tr>
<tr>
<td>Using complex passwords (contain letters, numbers, and symbols)</td>
<td></td>
<td>1.044</td>
<td></td>
</tr>
<tr>
<td>Using a different password for each different online account</td>
<td></td>
<td>1.302*</td>
<td></td>
</tr>
<tr>
<td>Deleting suspicious emails without opening them</td>
<td>1.033</td>
<td>1.777*</td>
<td>1.418</td>
</tr>
<tr>
<td>Logging out of websites when you are finished</td>
<td></td>
<td>0.718**</td>
<td></td>
</tr>
<tr>
<td>Adjusting website account settings (e.g. privacy settings)</td>
<td></td>
<td>1.280</td>
<td></td>
</tr>
<tr>
<td>Installing anti-virus or other security software, such as a firewall</td>
<td>2.062***</td>
<td>1.381*</td>
<td>0.689</td>
</tr>
<tr>
<td>Scanning computer regularly for viruses or other malicious software</td>
<td>1.599***</td>
<td>0.875</td>
<td></td>
</tr>
<tr>
<td>Protecting home wireless connection (wi-fi) with a password or been cautious using public wi-fi</td>
<td></td>
<td>0.916</td>
<td></td>
</tr>
<tr>
<td><strong>Constant</strong></td>
<td>0.068***</td>
<td>0.008**</td>
<td>0.008**</td>
</tr>
<tr>
<td>Cox &amp; Snell R Square</td>
<td>0.064</td>
<td>0.021</td>
<td>0.004</td>
</tr>
</tbody>
</table>

* = p ≤ 0.05  ** = p ≤ 0.01  *** = p ≤ 0.001

7.2 **Qualitative Analysis Findings**

Binary logistic regression results suggested that online activities had no influence on the risk of phishing victimisation. Voluntary and involuntary personal information disclosure emerged as two themes which may be possible reasons for being a target of phishing. Social
Networking Sites (SNS), online advertising websites and free Wi-Fi providers appeared to be the most common platforms where respondents revealed their personal information.

“Probably, I received phishing emails due to social media. You sometimes click on an add. They ask your email address on shopping websites for a newsletter...I received some tax-related emails after posting ads. But I am quite visible.” (Participant D).

Selling goods online appeared to increase the risk of falling victim to phishing. Interviews suggested that email addresses and phone numbers posted on online advertisement websites enhanced internet users’ visibility to motivated offenders. This is in line with the findings of Williams (2015), who also found that online auction selling enhanced the odds of being a victim of identity theft.

“I posted an ad to sell my previous car. I posted an ad on X website. Only my cell phone number and email address were visible on the website.” (Participant E).

It seems that most participants did not perceive a significant threat stemming from sharing personal information to register for free Wi-Fi. This can be attributed to the relative insignificance of personal information provided, as most people are more vigilant about personal financial information (Bryce and Fraser, 2014). A trade-off between the risk of losing personal information and the benefits of free Wi-Fi may be another explanation for yielding personal information to network providers (Workman, 2007). Likewise, the results of Cheung et al. (2015) suggest that perceived benefits is a significant factor affecting self-disclosure.

“I sometimes use free Wi-Fi in an airport or in café. I think they do not ask for very important personal information, so I am not very worried about providing them.” (Participant G).
Involuntary personal information disclosure emerged as another reason for becoming a target of phishing. Participants acknowledged experiencing an increased volume of phishing attempts in the aftermath of data breaches of companies holding their personal information.

“I received many phishing emails, and they increased dramatically after the hacking of T... My email account seemed to be something like everybody in the world knows it.” (Participant H).

“So, what happened when G was hacked, somehow my card details were saved there. I never save my card details online... That website, G, saved my card details without my permission.” (Participant I).

Interviews with control group participants suggested that internet skills and paying close attention to the contents of email messages might prevent victimisation.

“I received many dodgy emails, the last one was really good, except they used my email address instead of my name. The email was very convincing; I nearly clicked on it. Because I was really worried about it. Then I said no, it is not my name.” (Participant B).

“I often get emails supposedly from banks, saying that bank accounts have a problem if I click on the link, they will try to sort it out. ... It was so easy to tell it was a scam.” (Participant C).

CSEW 2014/2015 did not measure online deviancy. The impact of engaging with online deviancy on the risk of experiencing cyber-enabled and cyber-dependent crime victimisation was explored through the interviews. Of the 32 participants, 18 acknowledged engaging with online deviant activities. Free streaming, peer-to-peer sharing, and watching pornography emerged to be the most cited online deviant activities.

“I sometimes watch movies from illegal sources. I used to use torrents to download movies or programs. I do not know how they could make me vulnerable because I never gave
my account details. But I guess there could be viruses, which came with torrents.” (Participant A).

A total of 12 of participants who accessed online deviancy were the victims of hacking and malware infection. These findings may be interpreted as the presence of a relationship between online deviance and experiencing malware infection and hacking victimisation, thereby providing support for H1b. This finding is in line with previous cyber-dependent crime victimisation research showing that accessing adult websites, illegal downloading and free streaming increased the risk of malware infection (Holt and Bossler, 2013; Leukfeldt, 2015) and hacking victimisation (Holt and Copes, 2010).

8. Discussion

Cybercrime victimisation has become an emerging and significant issue due to the increased volume of sophisticated cyberattacks targeting individuals, organisations, and governments. This article is an investigation into the causes of becoming a victim of cybercrime through a well-established theory: LRAT. Specifically, the impact of individuals’ online lifestyles on the risk of experiencing two forms of cybercrime (cyber-dependent and cyber-enabled crimes) have been explored. We also examined the relationship between accessing the internet through insecure connections and public access computers and the likelihood of experiencing cyber-enabled and cyber-dependent crime victimisation. The effectiveness of online guardianship measures in preventing cybercrime victimisation was also explored. Additionally, we critically evaluated the explanation power of LRAT in relation to two forms of cybercrime victimisation.

8.1 Key Findings

The results of the study generally yielded support for the hypotheses. It was found that while accessing government websites emerged as a risk factor for malware infection, buying
goods or services appeared to enhance the risk of hacking victimisation. Email/instant messaging/chat rooms had a strong effect on both malware infection and hacking victimisation (H1a). Additionally, engaging with online deviancy emerged as a possible explanation for malware infection and hacking (H1b). Peer-to-peer sharing, watching free adult content, and free streaming were the most cited online deviant activities.

Furthermore, voluntary personal information disclosure through online platforms, such as SNS or advertisement websites, and involuntary personal information disclosure via data breaches of large companies, emerged as the most significant causes of becoming a target of phishing. This was the novel contribution of this study. Illustrating the adverse impact of accessing the internet through public access computers and insecure Wi-Fi connections was another significant contribution (H2a, H2b). Contrary to expectations, the binary logistic regression analysis results indicated that guardianship measures such as installing anti-virus software or regularly scanning a computer increased the risk of facing cyber-dependent crime victimisation (H3). This result is in line with previous studies (Ngo and Paternoster, 2011; Reyns et al., 2016; Williams, 2015), yielding a positive relationship between guardianship measures and the risk of cybercrime victimisation. This result may be attributed to the cross-sectional design of CSEW 2014/2015.

8.2 Practical Implications

As noted above, demonstrating the relationship between personal information disclosure and phishing victimisation was one of the novel contributions of this study. Previous phishing studies mostly focused on the decision-making processes of individuals who are exposed to fear-provoking messages (Silic and Back, 2016; Williams et al., 2017; Wright et al., 2014). This study documented the reasons for being targeted by spear-phishing emails that contain the personal information of individuals. It appears that the low perceived severity of sharing personal information online renders internet users as suitable targets for phishers. It is
possible that users do not anticipate any threat from sharing email addresses or phone numbers on these platforms. Given that the administrators of SNS have little or no control over the posts (Khobzi et al., 2019), users should be informed about the possible adverse consequences of yielding personal information through public awareness programs. The perceived benefit of self-disclosure was another explanation for the association between voluntary personal information and phishing victimisation. Free Wi-Fi connections offered at public places and selling goods online emerged as incentives that decrease users’ threat perceptions, yielding support to the findings of Cheung et al. (2015) and Walsh et al. (2020). Policymakers may consider implementing regulations regarding limiting the type of information required to login to free Wi-Fi connections, and the sort of information disclosed in online auction websites, to reduce the risks of yielding sensitive information online.

Involuntary personal information disclosure, which is the outcome of data breaches of large companies, was another cause of being targeted by unsolicited emails. Although previous phishing studies explored individual-level risk factors (Jansen and Leukfeldt, 2016; Leukfeldt, 2015; Leukfeldt, 2014), this study for the first time demonstrated the impact of the macro-level risk factor on receiving spear-phishing emails. Compliance programs regulating the encryption of stored data may be an effective solution to the adverse consequences of data breaches (Miller and Tucker, 2017). Moreover, organisations experiencing data breaches should make the extent of the threat transparent. Customers whose personal details are stolen should be well-informed about potential risks to alleviate the risk of phishing victimisation.

Analysis of this research demonstrated the association between online purchasing behaviour, including music/film downloads, and the increased risk of facing hacking victimisation, supporting the results of Leukfeldt and Yar (2016), Pratt et al. (2010), and Reynolds (2013) who found a relationship between online shopping, malware infection and consumer fraud victimisation. Impulsive buying may be a possible explanation for this result. Empirical
evidence suggested that impulsive people tend to pay less attention to the online merchant and make hasty decisions while shopping (Pratt et al., 2010; Reisig et al., 2009; van Wilsem, 2013a). Hence, impulsive consumers run the risk of providing their financial details to bogus websites, thereby facilitating the hacking of their online accounts. This result suggests that users should be more wary while providing their financial details to online merchants. Checking trust signs and green padlocks can be effective precautions to differentiate between genuine and bogus websites. Shopping from trusted or well-known online traders may be another safeguarding measure.

Lastly, accessing the internet through insecure Wi-Fi connections and public access computers had a significant impact on the risk of experiencing cybercrime victimisation, replicating the results of Hutchings (2014) and Williams (2015). This result indicates that users should pay attention to online activities while accessing the internet through insecure connections or public computers. Refraining from online activities that require sensitive information disclosure (i.e. shopping, banking) may be a preventive action.

8.3 Theoretical Implications

Although previous cybercrime studies established the presence of a relationship between internet users’ activities and the risk of victimisation (i.e. Ngo and Paternoster, 2011; Pratt and Turanovic, 2016; Reyns and Henson, 2016), the results of these studies implied that online activities do not affect the risk of cybercrime victimisation for different types of cybercrime equally. For example, the results of Ngo and Paternoster (2011), who examined the determinants of seven types of cybercrime, illustrated that situational-level factors predicted only the probability of being harassed by an online stranger. Likewise, van Wilsem (2013b) compared the behavioural risk factors of hacking and harassment. His results illustrated that certain risk factors emerged as predictors of a specific type of victimisation (i.e. social media use only predicted harassment). This study was the first time that the
differentiating impacts of online behaviours on cyber-enabled (phishing) and cyber-dependent (hacking and malware infection) crimes victimisation were specifically examined. This research revealed that online behaviours only enhanced the likelihood of facing cyber-dependent crime victimisation. This result may be attributed to the modus operandi of perpetrators. Cyber-enabled crimes are more interpersonal in nature, and deception of internet users through socially engineered messages is key in the commission of cyber-enabled crimes (Chen et al., 2017; Halevi et al., 2015). However, cyber-dependent crimes heavily rely on technical subterfuge, such as infecting target computers or exploiting technological vulnerabilities (Almomani et al., 2013; Hutchings, 2013).

9. Conclusion, Limitations and Research Implications

A mixed methods research paradigm was adopted to explore the factors that render internet users vulnerable to online threats. CSEW 2014/2015 was utilised to test the hypotheses. Additionally, transcripts of 32 semi-structured interviews with victims of cybercrime and ten semi-structured interviews with non-victim internet users were analysed to understand the underlying reasons for facing cybercrime victimisation. The research indicated that individuals’ online behaviours facilitate cyber-dependent crime victimisation more than cyber-enabled crime victimisation.

Additionally, previous cybercrime victimisation studies utilising LRAT as a theoretical framework largely neglected the impact of macro-level factors on the risk of facing victimisation. To address this gap, electronic devices were included in the cybercrime victimisation models in the binary logistic regression analysis. Qualitative analysis findings suggested data breaches of large companies rendered individuals suitable targets for phishing attempts.
This research has several limitations that need to be addressed. First, CSEW 2014/2015 did not measure online deviance. Semi-structured interviews were utilised to address this pitfall. Future research may use nationally representative samples to examine the relationship between online deviant behaviours, cyber-dependent and cyber-enabled crime victimisation. Second, as noted above, we examined the impact of macro-variables on the risk of cybercrime victimisation. The results suggest avenues for future research. Future research may consider including more macro-level variables, such as Wi-Fi connections or mobile applications, in LRAT victimisation models.

Furthermore, the results of this study suggested that the application of online safeguarding measures increased the risk of victimisation. This result could be interpreted as the impact of a false sense of security, which increases the propensity to engage with risky online activities (Ngo and Paternoster, 2011). However, the cross-sectional nature of survey data, which failed to measure the temporal order of victimisation experiences and application of safeguarding measures, could be another explanation (Reyns et al., 2016). Future studies may consider adapting a longitudinal research design to evaluate the effectiveness of online guardianship measures.

Lastly, this study is one of the first pieces of research employing a mixed methods paradigm to explore the factors that make home users susceptible to cyber-enabled and cyber-dependent crimes. While the quantitative phase of the study tested the hypotheses via a nationally representative sample, which enabled us to generalise the results to a global context, the qualitative stage not only addressed the pitfalls of quantitative datasets, but also provided significant insight into cybercrime victimisation. We strongly recommend utilisation of the mixed methods research paradigm for future studies.

NOTES:
REFERENCES:


Brenner, S. W. (2010), *Cybercrime: Criminal Threats from Cyberspace*, Prager, USA.


Acknowledgements

The quantitative data analyzed in this study were provided by UK Data Service

Declaration of interest statement

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.