Crime Science

RESEARCH

Open Access

To SPB or not to SPB? A mixed methods analysis of self-protective behaviours to prevent repeat victimisation from cyber abuse

Zarina I. Vakhitova[1*], Rob I. Mawby[2], Clair L. Alston-Knox[3] and Callum A. Stephens[1]

Abstract

This paper presents the findings from a mixed-methods examination of self-protective behaviours (SPBs) adopted by victims of cyber abuse from the rational choice perspective. The data from a sample of the U.S. adults ($N = 746$), members of an online opt-in panel, were analysed to first distinguish the types of SPBs adopted by victims of cyber abuse using a thematic analysis of open-ended responses. We then identified the factors associated with an increased likelihood of adopting SPBs and the specific identified types of SPBs using logistic regression with Bayesian variable selection and a stochastic search algorithm. Of the six identified types of SPBs, adjusting privacy settings was the most commonly reported response, and improving security (e.g. changing passwords, etc.) was the least common SPB. Older victims who reported higher than the average perceived impact from victimisation, were abused by a stranger and experienced either surveillance of their online activities or multiple types of abuse, were significantly more likely to adopt an SPB. Our findings inform strategies for both Internet user education and for preventing cyber abuse victimisation.

Keywords: Cyber abuse, Self-protective behaviours, Repeat victimisation, Bayesian variable selection, Stochastic search algorithm

Introduction

The use of the Internet and telecommunication technologies to stalk or harass adult victims, referred here as *cyber abuse*, is both common and often serious (Bocij 2006). According to the recent study by the Pew Research Centre, over 40% of U.S. adults experienced some form of cyber abuse at least once in their lifetime (Duggan 2017); in fact, it is now more common than face-to-face stalking and harassment (Short et al. 2014). Furthermore, cyber abuse appears to be a global problem with studies from Canada, Portugal, Taiwan, Australia, Hong Kong among others reporting high rates of victimisation (Hokoda et al. 2006; Pereira et al. 2016; Statistics Canada 2016; Vakhitova and Reynald 2014; Wong et al. 2014).

Cyber abuse can take many different forms such as "name-calling, trolling, doxing, open and escalating threats, vicious sexist, racist, and homophobic rants, attempts to shame others, and direct efforts to embarrass or humiliate people" (Duggan 2017). Other behaviours, also classified as cyber abuse, include impersonating the victim, ordering unwanted goods and services for the victim (e.g. subscribing to online pornography sites), using key-loggers to control and monitor victims, and electronic sabotage (Bocij 2006; Phillips and Morrisey 2004; Wykes 2007). The defining feature of cyber abusive behaviours is their repeated nature. Although the majority of victims of cyber harassment experience less serious forms of cyber abuse such as being called offensive names, serious abuse including physical threats and sexual harassment also occurs (Duggan 2017).

*Correspondence: Zarina@Vakhitova.com
[1] Monash University, Clayton Campus, Menzies Building, 20 Chancellors Walk, Victoria 3800, Australia
Full list of author information is available at the end of the article

While the individual impact varies, the effect of cyber abuse on victims is often significant (Vakhitova et al. in press). Victimisation can affect many areas of victims' lives including their physical and mental health, financial status and overall well-being (Dreßing et al. 2014; Fissel 2018; Melander 2010; Sheridan and Grant 2007; Short et al. 2014, 2015; Tokunaga and Aune 2017; Worsley et al. 2016). Considering the potentially serious consequences of experiencing cyber abuse, victims are expected to be motivated to take some measures to prevent repeat victimisation, a situation where the same victim experiences another incident of victimisation of the same kind or very similar to the initial victimisation event, but in reality, only some victims do (Averdijk 2011). For example, only 40% of victims of cyber abuse in a study by Duggan (2017) blocked the person responsible for abuse from further online contact, deleted their social media profile or withdrew from an online forum. So, why is it that not all victims take measures to prevent repeat victimisation?

The research in self-protection against traditional forms of stalking and harassment is well-established and offers several empirically supported explanations for why the adoption of SPBs is not uniform (see, for example, Baum et al. (2009); Buhi et al. (2009); Gottfredson and Gottfredson (1988); Guerette and Santana (2010); Reyns and Englebrecht (2010); Thompson et al. (2018); Wilcox et al. (2007)). However, the systematic research in the area of self-protection against online forms of deviance, as pointed out by Nobles, Reyns, Fox, and Fisher (2014, p. 993)"has not developed to the point where patterns in responses to victimisation, including self-protective behaviours taken by the victim, have been clearly identified".

Understanding the nature of self-protection by victims is particularly important in the context of technology-facilitated deviance such as cyber abuse. The traditional forms of crime prevention may not be effective or even possible in cyberspace (especially those involving traditional policing strategies like random patrols, etc.), so knowing what victims do to self-protect and why sometimes they do not do it would be particularly valuable to anyone involved in developing policies around safe technology use. Thus, this study's aims are two-fold. First, we aim to further the development of a comprehensive classification of self-protective behaviours that victims of cyber abuse adopt to prevent repeat victimisation. Then, the second aim is to identify the factors associated with the adoption of SPBs by victims of cyber abuse.

To achieve our objectives, we analyse the data from a survey of U.S. adults, members of an online opt-in panel, using a mixed-method research design: we first use qualitative thematic analysis of open-ended responses to identify specific types of SPBs adopted by victims of cyber abuse to prevent repeat victimisation, and then model the adoption of SPBs using logistic regression with Bayesian variable selection with the stochastic search algorithm. In our modelling we were guided by the rational choice theory (Beccaria 1764; Becker 1976; Bentham 1789; Browning et al. 2000; Clarke and Cornish 1985; Cornish and Clarke 1986) explaining the adoption of SPBs as an outcome of victims of cyber abuse weighing up the advantages and disadvantages of adjusting their behaviour. Here, we argue that only if the benefits of taking some precautions (evasive actions) outweigh the costs will they adjust their online activities. Please note, by definition, cyber abuse is characterised by the repeated nature of offending behaviour. This makes measuring prevention of *repeat victimisation or re-victimisation* a particular challenge. Traditionally, repeat victimization, or re-victimization, has been defined as an event that "occurs when the same type of crime incident is experienced by the same—or virtually the same—victim or target within a specific period of time such as a year" (Weisel 2005). However, unlike the traditional forms of crime such as burglary or assault, where it is fairly easy to identify the initial and the repeat events, the same is not true for cyber abuse. Here, we argue that the adoption of self-protection against re-victimisation from cyber abuse does not have to occur straight after the very first initial event (e.g. the first abusive email, or the first comment posted on the victim's social media page). Instead, we believe, self-protection can occur at any point in the chain of abusive behaviours. So, for the purposes of this study, we examine any changes in the way victims interact with telecommunication technologies, occurring at any point after the very first instance of abusive behaviour targeting the same victim(s), motivated by the same grievance(s) and perpetrated by the same offender(s). Examples of such behaviours include changing passwords on social media accounts, blocking person(s) responsible for cyber abuse, withdrawing from participating in online forums, etc. Please also note, measuring the effectiveness of self-protective behaviours (i.e. whether these behaviours resulted in reduced risk of repeat victimisation) was outside the scope of this study.

Literature review

Types of self-protective behaviours against cyber abuse

Due to the relative novelty of the phenomenon, the scholarship on self-protection against cyber abuse is currently limited to just a handful of studies, which nevertheless provide an important foundation for further investigation (Duggan 2017; Fissel 2018; Nobles et al. 2014; Tokunaga and Aune 2017). Using a robust methodology and a large nationally representative sample of U.S. adults (N = 4248), Duggan (2017) found that as a reaction to cyber

harassment, victims were most likely to confront the person responsible online and unfriend or block that person from further online contact, report the person responsible to a website or online service, discuss the problem online to draw support for themselves, change a username, delete a profile or withdraw from an online forum. While informative, Duggan (2017) provided the respondents with a fixed list of possible types of self-protective behaviours, leaving the opportunity for some SPBs that victims adopt not being included in the analysis.

In contrast, Tokunaga and Aune (2017) employed a qualitative thematic analysis of open-ended responses describing various self-protection strategies–a research design that could, in principle, produce a comprehensive classification (taxonomy) of SPBs adopted by cyber abuse victims. The researchers analysed the data from a small ($N = 51$) non-probability sample of victims of cyber abuse recruited from undergraduate university students and users of two popular cybercrime-victims focused web sites [(CyberAngels and Women Halting Online Abuse (WHOA)]. The analysis identified seven management strategies: (1) avoidance, (2) active technological disassociation, (3) help-seeking, (4) negotiation/threat, (5) compliance/excuses, (6) technological privacy management, and (7) derogation. *Active technological disassociation*, which involves the use of technology to prevent future encounters with the offending person(s), for example, adjusting the privacy settings within the social media environment, was reported as the most effective strategy as perceived by the victims. While making a significant contribution to the literature on the types of SPBs routinely employed by victims of cyber abuse, due to the recruitment and sampling approaches employed in this study, some SPBs may have been omitted.

Theoretical explanations of self-protection

The research aiming to explain self-protective behaviours by victims is extensive and offers several possible explanations. For example, Protection Motivation Theory (PMT) (Rogers 1975), which explains self-protection as a function of the perceived severity of a threatening event, the perceived probability of the occurrence, or vulnerability, the efficacy of the recommended preventive behaviour, and the perceived self-efficacy is commonly employed within the Information Systems literature to explain self-protective behaviours by Internet users (see, for example, Tsai et al. 2016; Herath and Rao 2009). The original PMT was later modified to include costs and rewards as additional explanations of self-protective behaviours (Maddux and Rogers 1983). In criminological literature, a popular explanation of self-protection against crime, advanced by Gottfredson and Hindelang (1979), emphasised the role of the seriousness of the offence, offender's prior criminal record, and the victim-offender relationship (Akers and Kaukinen 2009; Fisher et al. 2003).

Both these approaches are clearly rooted in the rational choice perspective (RCT), which assumes that every person is a rational agent, who performs cost-benefit analysis to determine whether the action is worth pursuing (Beccaria 1764). The RCT predicts that the decision to pursue a particular course of action is more likely when the benefits outweigh the costs (Becker 1976; Browning et al. 2000; Clarke and Cornish 1985; Cornish and Clarke 1986; McCarthy and Chaudhary 2014). The RCT is a popular theoretical perspective commonly used to explain the criminal decision-making process (Loughran et al. 2011, 2016; Pickett et al. 2018, 2019; Wortley and Sidebottom 2017). However, being a general-purpose theory, it is suitable for explaining decision making by any rational actor, including that by victims. When applied to self-protection, RCT explains the non-uniform adoption of SPBs as a result of a cost-benefit analysis performed by the victim following the initial victimisation event. The theory asserts that the SPBs are more likely when the benefits of preventing repeat victimisation are perceived as higher than the costs of prevention (McCarthy and Chaudhary 2014).

As Skogan (1981, p. 37) argued, any SPB to prevent repeat victimisation is associated with some cost: "there is no such thing as cost-free crime avoidance", in a situation where the cost of SPB outweighs the anticipated cost of repeat victimisation, "it may be rational to choose to do nothing" (Skogan 1981, p. 37). To warrant an SPB, the prevention of victimisation should provide a benefit that is at least equal to or greater than the anticipated cost associated with a repeat victimisation event. This would suggest that everything else being equal, the more significant the victimisation event and the higher the perceived victim impact from it, the more likely the victim is to act to prevent repeat victimisation.

Predictors of self-protection against cyber abuse

The empirical research generally supports the expectation that those who experience more serious consequences of victimisation would be more likely to adopt SPBs (see, for example, Averdijk 2011; Buhi et al. 2009; Bunch et al. 2014; Reyns and Englebrecht 2010). This appears to be also true for online forms of deviance like cyberstalking (Fissel 2018; Reyns and Englebrecht 2010; Nobles et al. 2014). Using data from 2006 National Crime Victimization Survey's (NCVS) Supplemental Victimization Survey (SVS), Reyns and Englebrecht (2010) found that seriousness of the offence affected stalking and cyberstalking victims' decision to report their experiences to the police. In particular, cyberstalking victims were more likely to report to the police when they felt

intimidated or threatened, lost time at work, and experienced a financial loss, the factors all reflective of victim impact.

Similar to Reyns and Englebrecht (2010), Nobles et al. (2014) compared self-protection by stalking and cyberstalking victims. Using a nationally representative sample (USA), the researchers identified four critical predictors of reporting cyberstalking to the police: offence seriousness, operationalised as the presence of threats and physical attacks against the victim; duration of the incident; fear of crime; and self-identifying as a victim of crime. While distinct, all four of the factors identified in Nobles et al. (2014) reflect in some form the impact of cyberstalking on its victim: it is not unreasonable to assume that a one-off incident would produce less significant impact compared with a long-term pursuit. It is also likely that someone who experiences significant fear of crime and identifies as a victim of crime is more affected compared with someone who is not. It is important to mention here that 2006 SVS survey analysed in Nobles et al. (2014) included mostly offline–types of SPBs, such as taking time off from work or school, changing or quitting a job or school, getting a gun and so on, with only one technological SPB (changing email address) included in the survey. It is not clear whether the same trends could be observed with other cyber abuse behaviours.

Notably, the studies reviewed here focused on the differences in self-protective behaviours between online and offline stalking and harassment while conceptualising cyberstalking as one uniform type of crime. However, both cyber stalking and cyber harassment can be committed using different methods, for example, by sending threatening or disturbing messages via email or by monitoring one's activities on social media, or by posting private information about the victim online. It is not unreasonable to expect that some methods may be more hurtful than others and that some methods may be easier to prevent than others. For example, it may be that direct messages are perceived as less damaging compared with public messages. Likewise, it may be easy to block the person responsible for abuse on social media, but it may be more difficult to prevent the person from posting the victim's personal information online. No research to date has examined the effect of different methods of cyber abuse on the adoption of self-protective behaviours, which leaves a significant gap in our knowledge.

The present study

The review of the literature identified a gap in our understanding of the mechanism that explains the non-uniform adoption of self-protective behaviours to prevent repeat victimisation by victims of cyber abuse. To address this knowledge gap, this study aims to answer the following two research questions:

Research Question 1: What self-protective behaviours do victims of cyber abuse adopt to prevent repeat victimisation?

Research Question 2: Is there a relationship between different methods of cyber abuse experienced by victims and the adoption of self-protective behaviours?

In this study, the term cyber abuse is used as an umbrella term for such behaviours as cyber stalking and cyber harassment and is broadly defined as any behaviour that involves the use of technology to stalk and/or harass adult victims.

Methodology

To answer these research questions, we analyse the data from a large sample of U.S. adults, members of an online opt-in panel, Amazon's Mechanical Turk (MTurk),[1] that were surveyed about their experiences with cyber abuse victimisation. The research is designed as a mixed-method study. First, we identify specific types of SPBs adopted by victims of cyber abuse to prevent repeat victimisation using a qualitative thematic analysis of open-ended responses. Then we model the adoption of SPBs using logistic regression with Bayesian Variable Selection with the stochastic search algorithm.

Survey instrument

To collect the information about the experiences of our respondents with cyber abuse victimisation, an online questionnaire was designed using Qualtrics online platform. Questions were developed especially for this study. The survey took no longer than 15 minutes to complete (average 6 minutes). An online survey was selected for data collection as it allows relatively easy access to a large relatively diverse pool of potential respondents and is cost-effective.

[1] The survey was conducted in accordance with the ethical requirements of the Griffith University Human Research Ethics Committee (HREC) and complied with ethics guidelines set forth by the HREC recommendations. Ethics approval number: CCJ/07/14/HREC. Participants were informed that their data would be treated anonymously, no identifying information would be collected and they could withdraw from the survey at any time without providing a reason.

Sampling

The sample analysed in this study was drawn from an online opt-in panel Amazon's Mechanical Turk (MTurk).[2] The data collection took place between 19th of May 2017 and 19th of September 2017. We limited participation in the study to MTurk members who were at least 18-years-old (at the time of participating in this research) and who resided in the United States.[3] In total, 1623 respondents began the survey, and 1463, or slightly over 90%, completed the survey. The participants were offered a small monetary compensation for their participation in the research (a completed survey). Only fully completed surveys were included in the final dataset analysed in this paper.

The biggest advantage of samples from online opt-in panels like MTurk is that it allows access to a large and fairly diverse pool of potential respondents (Behrend et al. 2011). The breadth and the variability of the sample are particularly important for our study as our goal here was not necessary to measure the prevalence or exact proportions of particular behaviours within the general population but instead to obtain as complete nomenclature as possible. The disadvantage, of course, is the non-probability nature of MTurk panel with all the attendant potential for the collected sample to be biased. However, while our sample is not representative of the U.S. adult population, we can still obtain useful insights into the types of activities victims undertake to prevent repeat victimisation even if the proportions and frequencies of specific behaviours may not reflect the reality particularly well.

To identify victims of cyber abuse among those who accepted our invitation to participate in the survey, we first asked all our respondents whether they ever experienced any form of cyber abuse. We provided the respondents with a definition of cyber abuse and examples of behaviours that classify as cyber abuse.[4] Of the total number of respondents, around half ($N = 746$) reported experiencing some form of cyber abuse. Only those respondents who reported experiencing at least one method of cyber abuse were included in the sample analysed herein.

Measurements

To identify victims who adopted SPBs to prevent repeat victimisation from cyber abuse and the specific types of SPBs, we asked our respondents whether experiencing cyber abuse caused them to change the way they use technology, and if yes, how exactly. The answers to the first question were coded into a binary variable SPB (1 = adopted, 0 = not adopted), which was used in the quantitative analysis to identify the factors associated with the adoption of SPBs (RQ2). The open-ended responses were analysed using a thematic analysis procedure to identify specific types of SPBs (RQ1).

The literature review suggests that seriousness of crime/deviance and nature of the relationship between the victims and the abuser may be important explanations of the adoption of SPBs. In this study, we measured two proxies of the seriousness of cyber abuse victimisation. First, we measured the perceived impact of crime [Imp] on the victim by asking our respondents how affected they were by the incident they experienced psychologically, emotionally, financially, or otherwise. To answer this question, the respondents picked a position on a slider anywhere between 0.0 and 2.0 (1 decimal place) where 0.0 meant the respondent was not at all affected by the abuse, 1.0—somewhat affected and 2.0—profoundly affected. Please note, we did not include any follow-up questions on how victims were affected. And second, we measured the number of different methods of cyber abuse [N of M] experienced by the victim within one incident. To be considered as belonging to one incident of abuse all methods experienced by the victims must have been motivated by the same source, perpetrated by the same individual(s), and within a limited time frame.

To measure exposure to specific methods of cyber abuse, the respondents were asked to think about the most recent or most memorable incident they

[2] MTurk has been widely used by social scientists, including criminologists (see, for example, Denver et al. 2018; Enns and Ramirez 2018; Gottlieb 2017; Groenendyk 2016; Pickett and Bushway 2015; Vakhitova et al. 2019; Vaughan et al. 2019). Criminologists employed MTurk samples to examine such diverse and important topics as public support for private prison and immigration detention facilities, capital jurors' sentencing decisions, and public attitudes toward criminal justice reform for nonviolent offences.

[3] The text of the invitation to participate stated: "You are invited to participate in the survey that aims to identify the situational factors associated with cyber abuse. Cyber abuse involves the use of the Internet or other technological means (cell phones, gaming devices, etc.) to stalk or harass others. It can take forms of emails, texts (SMS), posts on blogs, online forums and social media pages of a persistent, annoying, alarming or threatening nature."

[4] The following is the text of the question used to identify victims of cyber abuse: *Have you ever experienced any form of cyber stalking or cyber harassment directed at your personally? By cyber stalking and cyber harassment, we mean the use of the Internet or other technological means (cell phones, gaming devices, etc.) to stalk or harass. It can be in the form of emails, texts (SMS), posts on blogs, online forums and social media pages of a persistent, annoying, alarming or threatening nature; monitoring your daily activities using social media or specialized software; posting information about your online (photos, documents, videos) without your consent or distribution such information to others via email, SMS or other technological means; impersonating you online or through email or SMS; subscribing you online to unwanted services, products, activities, etc. or other similar behaviours.*

experienced[5] and to select one or more specific behaviours they experienced from the list: (1) you received a text message, email or a private message via social media addressed to you personally (Method 1); (2) someone posted derogatory, embarrassing information (documents, photos, videos, etc.) about you on the Internet or distributed it to others via email, text (SMS) or other technology or someone created a website or a social media page containing derogatory or embarrassing information about you (Method 2); (3) you were subscribed to unwanted services, products, activities and you only found out about the subscription after you started to receive the services or products or were invited to participate in the activities (Method 3); (4) someone, pretending to be you, sent email or text messages or private messages on social media pages to your family, friends, co-workers, or other third parties (Method 4); (5) your daily activities were monitored by someone via social media or a tracking software (Method 5). The answers to this question were used to create five *Methods of abuse* variables.

To control for the potential effect of demographic characteristics on the adoption of SPBs suggested in previous research, we also collected information about our respondents' age, gender (0 = male, 1 = female), race (0 = non–white, 1 = white), and employment [Emp] (0 = unemployed, retired or a student, 1 = employed full time or part-time). We also asked our respondents whether they knew their abuser before abuse or whether they were abused by a stranger [OVR] (0 = did not know abuser, 1 = knew abuser).

Descriptive statistics

A total of 746 respondents in our sample experienced some form of cyber abuse (51%). These respondents were included in the sample analysed herein and are described in Table 1. On average, our respondents were quite young (mean age of 35 years) and predominantly female (52%), white (73%) and employed (80%). The most common method of abuse was direct abusive messages ($N = 508$), and the least common–impersonating the victim online or through email or texts ($N = 130$). On average, victims experienced 1.7 methods of abuse in one incident with most experiencing only one method (see Fig. 1).

The majority of cyber abuse incidents described by our respondents occurred in the context of a prior offender-victim relationship ($N = 562$; 74.9%). The average impact reported by the victims was around 1.13 (out of max 2.00) (SD = 0.6), which can be interpreted as only slightly

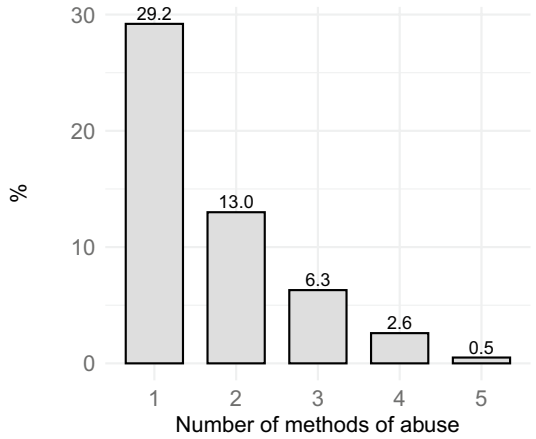

Fig. 1 Proportions of victims who experienced one or more method of abuse within one incident

higher than "somewhat affected". Around 40% of victims of cyber abuse in our sample reported adopting at least one form of SPB following as a reaction to victimisation ($N = 308$, 41.3%). This is not dissimilar to findings in Duggan (2017) and Nobles et al. (2014), which employed samples, representative of the U.S. population. Please note that many victims adopted multiple SPBs within one incident of cyber abuse, which is reflected in the analyses presented in this paper.

Analytic strategies

To answer Research Question 1 we have conducted a qualitative thematic analysis of open-ended responses of victims about self-protective behaviours they adopted following cyber abuse victimisation. To answer Research Question 2 we have conducted several exploratory data analyses followed by modelling using logistic regression with Bayesian variable selection and stochastic search algorithm implemented in AutoStat®.

Thematic analysis

The purpose of thematic analysis was to identify patterns reflective of the crime prevention mechanism of SPBs adopted by victims of cyber abuse. An approach similar to that recommended by Braun and Clarke (2006) was followed, comprising the following steps: (1) carefully reading the responses to familiarise ourselves with the data, (2) generating and applying the initial codes by documenting the apparent patterns, ((3) combining the initial codes into overarching themes, (4) reviewing the original interview data to make sure the identified themes adequately represent the data, (5) defining the themes, and finally (6) selecting themes relevant to the research questions and most representative of the data

[5] We asked our respondents to focus on the most recent or most memorable event in order to avoid potential memory and recall issues and ensure respondents are able to provide enough detail about the event.

Table 1 Descriptive statistics of the sample ($N_{victims} = 746$)

Variable	*SPB*		*No SPB*		*All victims*	
	N	%	*N*	%	*N*	%
Cyber abuse impact						
Victim impact ($\mu(SD)$)	1.36	(0.5)	0.98	(0.6)	1.13	(0.6)
Demographic characteristics						
Age ($\mu(SD)$)	32.7	(11.4)	30.3	(25.0)	31.2	(20.6)
Gender (female)	189	61.4	217	48.4	405	53.7
Race (white)	216	70.1	316	70.5	532	70.7
Employment (employed)	249	80.8	356	79.5	603	80.7
OVR[a] (prior)	211	68.5	356	79.5	565	74.9
Method of cyber abuse						
M1. Direct abusive messages	206	40.7	300	59.3	506	67.1
M2. Indirect abuse posted online	103	40.7	150	59.3	253	33.6
M3. Subscription to unwanted services	92	42.2	126	57.8	218	28.9
M4. Impersonation online	68	52.3	62	47.7	130	17.2
M5. Surveillance of online activities	99	61.9	61	38.1	160	21.2
Number of methods of abuse ($\mu(SD)$)	1.85	(0.9)	1.57	(0.9)	1.68	(0.9)

[a] Offender-victim relationship

to be included in this paper and checking whether these selected themes are representative of the data as a whole. As recommended in Braun and Clarke (2006), a reflective journal was used in the initial steps of the analysis to aid in coding. Table 4 (see Appendix A) contains an illustration of the entries in the journal and how they aided in developing the initial codes and the final themes.

To get as complete a picture of SPBs as possible, we analysed three groups of textual responses: (1) responses describing SPBs ($N = 302$; $\mu = 12$ words; range 1 to 102 words), (2) responses describing the actual cyber abuse event ($N = 288$; $\mu = 44$ words; range 3 to 196 words) and, finally, (3) responses describing the overall effect of the event on the victim ($N = 682$; $\mu = 30$ words; range 1 to 373 words). The coding was performed using an MS Excel spreadsheet by two independent coders with Krippendorfs's α coefficient of inter-rater agreement of 0.78 (substantial) (Krippendorff 2013). When the coders disagreed, they talked to each other to come up with a mutual decision on how to code a case.

Logistic regression with Bayesian variable selection

To identify the factors associated with the increased likelihood of adopting SPBs to prevent repeat victimisation from cyber abuse, we modelled the mechanism using a binary logistic regression with Bayesian variable selection and stochastic search algorithm implemented in AutoStat®. The full model likelihood for a logistic regression, where there are k potential explanatory variables, can be specified as

$$\text{logit}(y) \mid \beta, X, \sigma^2 \sim N(\beta_K X, \sigma^2 I)$$

where $K = \{0, 1, 2, \ldots, k\}$ possible regressors (K = 0 indicates intercept term).

In deciding on the modelling approach, we took into consideration the exploratory nature of the study, the lack of theoretical guidance on exact model specification, and the benefits of statistical methods of variable selection identified in previous literature (see, for example, Raftery (1995); Vakhitova and Alston-Knox (2018); Vakhitova et al. (2016)). In the absence of previous research or strong theory, rather than treating only the model parameters as being subject to uncertainty, the model itself can also be associated with uncertainty. This approach, known as Bayesian model averaging, is a variable selection technique that treats the model as uncertain and produces a posterior distribution for the model coefficients that is averaged over a series of models, based on parameter inclusion and the probability of each model Ando (2010). Posterior distributions for coefficients for individual models are not examined in detail, as they are prone to be over-estimated in magnitude, and elude to greater effects than are reliable in future studies. Bayesian model averaging produces robust parameter estimates that are less prone to exaggeration and over-confidence in the variable affect (Hoeting et al. 1999; Madigan and Raftery 1994), and as such, the inferences from this model yield greater average predictability of the results in future studies. Importantly, this model structure does not require researchers to remove terms from the model, as coefficients associated with variables that have a minimal

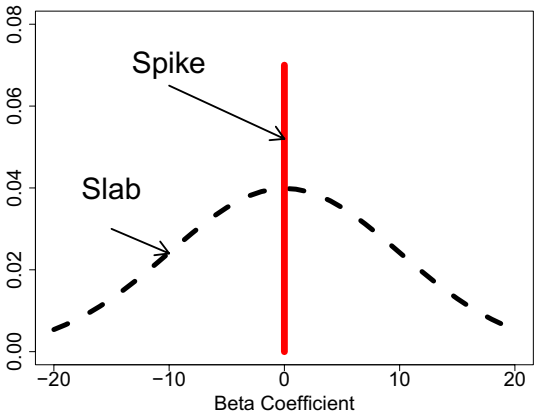

Fig. 2 Spike-slab algorithm

inclusion probability are shrunk towards zero, and as such, leaving them in the model has little impact on subsequent predictions.

As the number of parameters in the full model increases, the number of potential models can increase dramatically, with 2^k possible combinations. It is not feasible to always examine every potential model when data sets have large numbers of explanatory variables. A stochastic search algorithm is used to search the model space and determine the most likely models that can explain the outcome as well as preserving good estimation performance (Marin and Robert 2014). This approach also replaces the use of a p-value (using a Wald statistic or a measure of model fit) with an inclusion probability. This inclusion probability is based on the number of models in which the parameter is included and how probable these models are deemed. To estimate these models, we employed AutoStat® (http://pa-group.com.au/autostat.php).

In a Bayesian setting, the unknown parameters, β require a prior distribution to be specified to estimate their respective posterior distributions, based on the MCMC samples. In this study, we employed a G-prior (spike-slab) to enable the variable selection. A schematic diagram of the G-prior spike slab is shown in Fig. 2, indicating that the prior can take 2 states. During MCMC iterations where the coefficient is included in the model (as indicated by the stochastic search algorithm), the prior used in this posterior sample draw will be a G-prior, indicated as the "slab". Similarly, for iterations when the stochastic search does not include a coefficient, the prior used in the posterior draw is a point mass at zero (0), indicated by the "spike", resulting in a posterior draw of the coefficient that is exactly zero (0).

The g-prior (slab) for our β parameters is given by: [6]

$$p(\beta \mid y) \sim MVN(0, g\sigma^2(X^TX)^{-1})$$

As g decreases, the prior becomes more concentrated around zero (0) and takes on a more active role in the posterior distribution specification. In this example, we set g to be equal to the sample size (the default value in AutoStat©). For more information about the stochastic search algorithm for variable selection, and this specification of the g-prior, please see Marin and Robert (2014).

The results

Research Question 1: What types of self-protective behaviours do victims of cyber abuse adopt to prevent repeat victimisation?

Our analyses revealed six types of SPBs victims of cyber abuse adopt to prevent repeat victimisation.

SPB 1: Adjusting privacy settings

A relatively large proportion of victims who realised they were being stalked or harassed online adjusted their privacy settings ($N = 103$; 13.8%). This type of SPB involves adjusting privacy settings on social media platforms such as Facebook by specifying who can see one's profile information and posts. For example, it is possible to limit the circle of people who are allowed to see the posts to friends only. This SPB may be particularly effective when the person(s) responsible for abuse is a stranger.

> *[R0036]: I use maximum privacy settings now. When I realized this person was stalking me, I changed all the privacy settings in all of my accounts to maximum privacy.*

This SPB is technically quite straightforward and does not require much effort. Adjusting the privacy settings allows leaving the victim's information online while making it visible to those trusted only:

> *[R0131]: I limited posts to just be visible to friends only.*

Overall, this SPB allows limiting the visibility of one's content to a smaller circle of trusted friends without limiting one's online activities.

SPB 2: Blocking specific contacts

This SPB is used when the source of the abuse is identified ($N = 73$; 9.8%). It allows the victim to reduce access to herself by one or more specific individuals while still participating in online discourse and sharing the information with those trusted ones. The most common situation where blocking/deleting contacts is used is in the

[6] MVN–multivariate normal.

case of intimate partner relationship, specifically, after break up of a relationship:

> *[R0029]: My ex would send messages from a fake account to make me angry... I let it go and just blocked those fake accounts as well as hers.*

Intimate partner relationship is not the only context in which victims employ blocking the offending contact as a self-protection measure. Expressing one's political views could make you a target for those not sharing your views:

> *[R0558]: I am a visual artist and sometimes post my political and social views on my social media pages. A woman ... seemed very upset and angry toward me and began sending me messages telling me I was going to hell, and that I am liberal trash and a horrible person. She stalks all my websites and makes sure I am aware of her presence and opinion. She sometimes takes my images and edits them scratching out parts and posts them on an anonymous page... I am more careful about letting just anyone follow me.*

It appears that blocking offending contacts on its own may not be effective though, and therefore many victims utilise SPBs aiming to reduce one's accessibility in combination with other SPBs:

> *[R0586]: I blocked her number and profile. I also made my Facebook private, and only those who are friends with my friends can see my profile.*

Blocking specific contacts (SPB 2) is different to adjusting privacy settings (SPB 1) in that it is more targeted and is less restrictive by allowing strangers to see one's content and only blocking specific individuals believed to be responsible for the abuse. Both adjusting privacy settings and blocking specific contacts aim to reduce one's visibility to potential abusers.

SPB 3: Improving security

Another common strategy employed by victims to prevent repeat victimisation involves a variety of security measures such as changing passwords, installing antivirus and/or firewall software ($N = 42$; 5.6%).

> *[R0341]: After the incident I took precautions to prevent further instances from happening by changing many of my passwords and being more selective about who I provided my information to.*

The difference between this measure and the measures reducing visibility is that the increased security does not necessarily change the visibility of the information, but it does affect the way third parties can interact with said information:

> *[R0159]: I disabled comments on my posting across the platform.*

Interestingly, for some, experiencing cyber abuse prompted learning new skills or improving general security awareness, including how to use a passcode on a phone or block certain phone number:

> *[R0183]: I became more informed on the importance of implementing privacy settings on social media.*

Unlike adjusting privacy settings (SPB 1), improving security aims to restrict access to the victim and his/her information rather than make the victim less visible online.

SPB 4: Self-censorship

In our sample around 8% of victims of cyber abuse reported restricting their online discourse by avoiding sharing their political or other views on contentious topics to reduce the chance of repeat victimisation ($N = 57$; 7.6%). This is a particularly interesting type of self-protective behaviour reported by the victims which involve self-censorship, or conscious withholding of one's true opinion from an audience perceived to disagree with that opinion (Hayes et al. 2005; Williams 2002). The phenomenon, also known as the "spiral of silence", has been first described by the political science researcher Noelle-Neumann (2006). Though not yet discussed in the context of self-protection from crime (in particular, from cyber abuse), a recent study by Pew Research Centre found this phenomenon is observable in online as well as in offline environment and the respondents who used social media such as Facebook were more willing to share their views if they thought their followers agreed with them (Hampton et al. 2014).

> *[R0544]: I usually don't state my political views online, because I'm really not interested in getting into disagreements with people who are hiding behind a computer. However, I calmly made a comment about a policy that I agreed with, and a stranger made nasty comments to my post and also sent me direct messages telling me that I was stupid and many other verbal insults... I went back to keeping my opinions to myself. If people aren't adult enough to discuss both sides calmly, I'm not interested in debating with strangers.*

Interestingly, oftentimes, in line with Finkelhor and Asdigian (1996), the cause of abuse is not in what the victims do, but who he/she *is*. In these instances, self-censorship by itself may not be enough and the only way to stop the abuse may be a partial or complete withdrawal from the online discourse.

[R0412]: I started playing violent online multiplayer games less often and will purposefully avoid revealing my race when communicating with others online... I was always ridiculed for my dialect and my accent online, and was only rarely insulted specifically for my race, political, or religious beliefs. In recent years, however, the amount of racially motivated insults and discrimination on my religious beliefs has begun to overwhelm me and negatively [a]ffected my interactions with others online. Often times people will insult my race and religious beliefs not knowing that they are also insulting me, and when I raise the issue with them I am only insulted more and others seem to tolerate the action. The increase in hate and harassment online has naturally deterred me from playing and socializing with many people online and I now tend to only communicate with others I know or in cooperative or non-violent games.

In contrast to the first three discussed SPBs (i.e. adjusting privacy settings, blocking specific contacts and improving security), this SPB does not involve any management of technology used to facilitate the online discourse. No settings are adjusted and no new software is used. Instead, this SPB is all about adjusting one's behaviour concerning the use of technology.

SPB 5: Avoiding sharing personal information online

Sharing sensitive personal information can make one vulnerable to an attack. It is this sensitive information that some online abusers seem to crave. Therefore, victims who experienced abuse as a result of sharing such information online may employ this type of SPB to prevent repeat victimisation ($N = 43$; 6.8%):

[R0097]: The online community I was part of seemed like a safe, relatively isolated place, so a group of people finding my photos and posting them on their own forum to make fun of was very jarring. They were making fun of me for being fat, and it surprisingly didn't really hurt my self-esteem but it did make me retreat from being as public online. I basically stopped being an open member of the community and became a lot more anxious while being candid online.

Essentially, this SPB involves the victim restricting access to his or her private information (e.g. photos, documents, etc.) by not posting it online. This SPB is similar to self-censorship as both involve restricting the behaviour of the victim, however, these two SPBs are distinct as the types of information potentially shared online are different (personal opinion vs. private information) and therefore, the types of abusers that may find these different types of information "attractive" and therefore, the general mechanism of victimisation are likely to be different too.

SPB 6: Avoiding technology/social media

The final identified SPB is related to removing oneself from the environment in which the victim was initially abused or, at least reducing one's presence in that environment ($N = 60$; 8.0%). Considering that the Internet and social media have become an integral part of the modern social life and completely disconnecting from it would be difficult and for some impossible, it is not surprising that this, the most radical type of SPB is not particularly popular.

[R0223]: [N]ow I don't spend as much time online as I used to.
[R0710]: I got off the dating site.
[R0974]: I closed my online public accounts and screen all of my phone calls. I won't participate in any online forums or chatrooms or social media.
[R1088]: Shut my phone off much more often.
[R1171]: I am not on any social media websites anymore.
[R1194]: I stopped or slowed my online activities quite a bit.

While appearing as the most extreme and therefore the most effective SPB to prevent repeat victimisation, the emergence of new methods of cyber abuse that do not involve the victim directly (see, for example, research on indirect cyber abuse (Vakhitova et al. 2018)) and, therefore, do not require that the victim is present online mean that even the complete disengagement from any time of online activities, including the participation in online discourse, do not guarantee the absence of repeat victimisation.

To summarise, the majority of victims (62%) did not change the way they use technology following an incident of cyber abuse victimisation. Of those who did, nearly a third (27%) reported only one type of SPBs and less than 2% reported 3 or more SPBs. Of those who reported adopting at least one type of SPB, the most common SPB in our sample was *SPB 1–adjusting privacy settings* (13.8%), and the least common *improving security* (5.6%) (see Fig. 3).

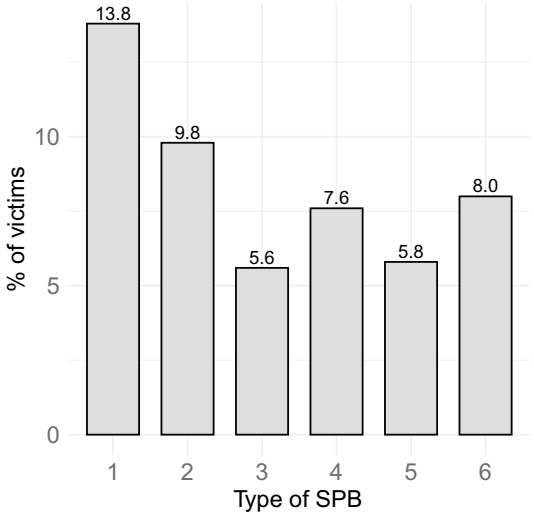

Fig. 3 Summary of SPBs reported by victims of cyber abuse ($N = 308$), where, 1–adjusting privacy settings; 2–blocking contacts; 3–improving security; 4–self-censorship; 5–avoiding sharing personal information; 6–avoiding technology/social media

Research Question 2: What factors are associated with self-protective behaviours against cyber abuse?

Table 2[7] presents correlation coefficients for bi-variate relationships for all variables of interest in this study. The coefficients suggest that all methods of abuse are correlated with SPBs. No matter the method, adjusting privacy settings (SPB 1) and avoiding technology/social media (SPB 6)–appear to be a popular option for most victims. Other SPBs appear to be more method of abuse-dependent: SPB 2–blocking contacts–does not seem to be used often by victims of indirect abuse posted online (Method 2) and those who were subscribed to unwanted goods/services. This seems logical considering neither of these methods involves a direct offender-victim contact where blocking the offender could be an effective strategy. Similarly, SPB 3–improving security–is not used by those who are abused indirectly (Method 2) basically for the same reasons discussed earlier. Notably, SPB 4–self-censorship is also not used by victims who were subscribed to unwanted goods/services and who were impersonated online. Overall this suggests that victims generally adopted the SPBs that were most appropriate for responding to the types of cyber abuse they experienced.

[7] Spearman's rho coefficient was calculated for the pairs of continuous variables (e.g. victim impact and age), point-biserial correlation coefficients were calculated for continuous-dichotomous variable pairs (e.g. Age and Method 1), and Phi coefficients for pairs of dichotomous variables (Method 1 (direct abusive messages) and SPB 1 (maintaining privacy)).

Figure 4 suggests victims who reported adopting SPBs were more likely to report higher than the average impact from abuse compared to victims who did not adopt any SPBs. This is in line with previous research that identified the seriousness of crime as an important factor explaining SPBs.

Further, Table 2 suggests that different types of SPBs are associated with different levels of victim impact. It appears that victims who experience higher levels of perceived impact are more likely to adopt SPB1 (adjusting privacy settings), SPB5 (avoiding sharing personal information) and especially SPB6 (avoiding technology/social media), while SPB4 (self-censorship) is not significantly associated with victim impact. Their ease of execution and availability may explain why these types of SPBs are the most popular.

Another proxy for the seriousness of crime measured in this study was the number of different methods of abuse victims experienced as part of one incident. It would not be unreasonable to expect that the higher the number of methods, the more intense and therefore more serious the abuse would be. As Fig. 5 shows, as the number of methods of abuse goes up (there are only 2 respondents who reported experiencing all 5 different methods of abuse in one incident), the proportion of victims who adopted at least one method of abuse goes up. A similar trend can be observed when we look at the number of SPBs victims adopt as a function of the number of methods of abuse they experience.

Figure 6 suggests that the relationship between the number of SPBs adopted by the victim and the number of methods of abuse experienced by the victim is not linear. This observation may be explained by the fact that in our sample there are very few victims ($n = 45$) who experienced more than 3 methods of abuse and not one victim who adopted more than 3 SPBs. Having a larger sample could help establish the stability of this observation.

Figure 7 shows the proportions of victims of different methods of abuse who adopted specific types of SPBs. Several things are clear. First, the most popular type of SPB is adjusting privacy settings (SPB 1), and Method 5 (surveillance of online activities) has the highest proportion of victims who adopted at least one type of SPB. Figure 7 and Table 2 suggest a relationship between the methods of abuse and the type of SPBs adopted by victims. In particular, victims who experienced direct abusive messages (M1) were more likely to adjust their privacy (SPB1), block the person responsible for the abuse (SPB2) or self-censor (SPB4), and less likely to improve security (SPB3). In contrast, victims who experienced subscription to unwanted good/services (M3) were most likely focus on improving their security (SPB3), but not likely to try to block the person responsible (SPB2)

Table 2 Correlation matrix

	SPB1	SPB2	SPB3	SPB4	SPB5	SPB6	M1	M2
SPB2	0.20[b]							
SPB3	0.06[a]	0.07[b]						
SPB4	0.03	0.07[a]	0.03					
SPB5	0.11[b]	0.07[b]	0.09[b]	0.17[b]				
SPB6	0.06[a]	0.08[b]	0.07[a]	0.05	0.11[b]			
M1	0.22[b]	0.22[b]	0.08[b]	0.18[b]	0.14[b]	0.14[b]		
M2	0.17[b]	0.02	0.04	0.08[b]	0.09[b]	0.08[b]	0.19[b]	
M3	0.10[b]	0.05	0.16[b]	0.05	0.06[a]	0.09[b]	0.18[b]	0.18[b]
M4	0.12[b]	0.07[b]	0.13[b]	0.01	0.07[b]	0.13[b]	0.15[b]	0.18[b]
M5	0.21[b]	0.10[b]	0.14[b]	0.12[b]	0.19[b]	0.18[b]	0.18[b]	0.19[b]
Age	− 0.09[b]	− 0.04	− 0.00	0.02	− 0.04	− 0.04	− 0.30[b]	− 0.20[b]
Gender	0.11[b]	0.06[a]	0.01	− 0.01	0.05	− 0.02	− 0.01	− 0.04
Race	0.02	− 0.05	− 0.03	0.00	− 0.01	− 0.03	− 0.02	− 0.06[a]
Empl	0.00	0.04	0.01	0.04	0.02	− 0.00	0.00	0.01
OVR	− 0.03	− 0.01	− 0.13[b]	− 0.10[a]	0.00	0.07	0.02	0.13[b]
Impact	0.15[b]	0.09[a]	0.08[a]	0.06	0.14[b]	0.20[b]	0.01	0.12[b]
N of M	0.29[b]	0.21[b]	0.17[b]	0.19[b]	0.19[b]	0.21[b]	0.73[b]	0.55[b]

	M3	M4	M5	Age	Gen	Race	Empl	OVR	Imp
M4	0.25[b]								
M5	0.24[b]	.14[b]							
Age	− 0.14[b]	− 0.13[b]	− 0.07[b]						
Gender	− 0.06[a]	− 0.05[a]	0.02	0.10[b]					
Race	− 0.10[b]	− 0.07[b]	− 0.04	0.20[b]	0.03				
Empl	− 0.00	− 0.02	0.00	0.14[b]	− 0.13[b]	− 0.03			
OVR	− 0.06	− 0.11[b]	0.05	− 0.19[b]	0.01	0.04	0.02		
Impact	0.02	0.09[a]	0.13[b]	− 0.03	0.14[b]	− 0.01	0.01	0.16[b]	
N of M	0.54[b]	0.43[b]	0.47[b]	− 0.35[b]	− 0.05	− 0.08[b]	0.01	0.02	0.16[b]

[a] Correlation is significant at the 0.05 level (2-tailed)

[b] Correlation is significant at the 0.01 level (2-tailed)

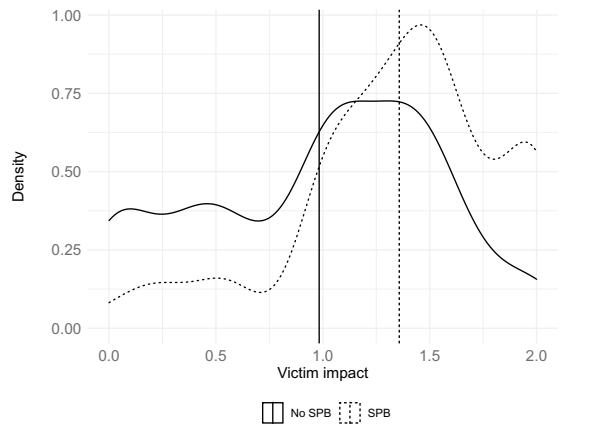

Fig. 4 Probability density plot of victim impact associated with adopting or not adopting SPBs

(probably because the identity of the abuser is unknown). Victims who experienced surveillance (M5) were most likely to adjust their privacy settings (SPB1), avoid sharing personal information online (SPB5) or avoid the Internet altogether (SPB6). Those who experienced being impersonated online (M4) were most likely adjust their privacy settings (SPB1), improve their security (SPB3) or avoid using the Internet (SPB6).

Table 3 presents the top five best models for explaining the mechanisms of adoption of SPBs against cyber abuse using Bayesian variable selection analysis,[8] as well as the posterior means and standard deviations for each coefficient. The best models are presented in terms of their probability of providing the best explanation for SPBs. The coefficients are presented in the order of their

[8] Number of iterations performed, excluding burnin: 10,000; burnin: 1000.

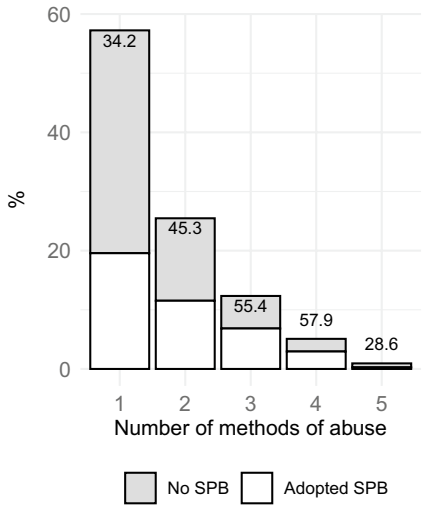

Fig. 5 Proportions of victims who adopted SPB(s) as a function of number of methods of abuse victim experienced

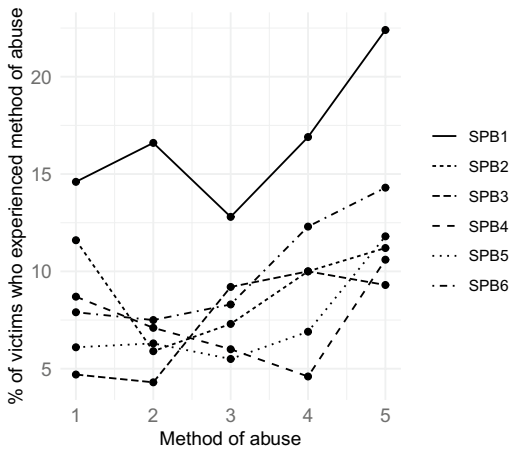

Fig. 7 Proportions of victims of different methods of abuse who adopted different types of SPBs. Here, 1 is adjusting privacy settings; 2–blocking contacts; 3–improving security; 4–self-censorship; 5–avoiding sharing personal information; 6–avoiding technology/social media

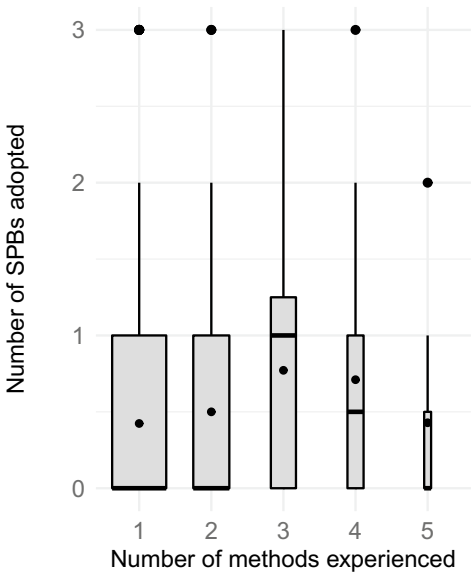

Fig. 6 Proportions of victims who experienced multiple abuses and adopted multiple SPB(s)

associated probability of inclusion, which reflects the importance of their contribution to the overall explanatory model.

The top five models have a cumulative posterior probability of nearly 60%, suggesting that the rest of the plausible models are much less likely and warrant no further investigation. Notably, the first best model (posterior probability = 24.3%) is nearly twice as likely as the second-best model (posterior probability = 13.2%). Based on the best model (Model 1) we conclude that victim's age, method of experienced abuse, level of impact and the nature of offender-victim relationship all appear to be important predictors of SPBs. Specifically, victims who experienced surveillance of their online activities were 3 times more likely to adopt SPBs than those who did not experience this method of cyber abuse. Of the other methods of cyber abuse, only being impersonated online provides a reasonable explanation of adopting SPBs, however, its inclusion probability is well below 50%, suggesting that it does not contribute to the explanation as actively as, for example being monitored online, which has an inclusion probability of 100%. Further, with each unit of increase in victim impact, the chances of adopting SPBs increase nearly 5-fold ($OR = 4.80$), meaning that someone who has reported the impact is 2.00 (profoundly affected) is nearly 5 times as likely to adopt an SPB compared with someone who reported impact of 1.00. Further, victims who did not know their abuser were more than 2 times ($OR = 2.24$) likely to adopt SPBs compared with those who knew their abuser. And finally, with each additional year of age, the chances that the victim adopts an SPB increase by 3% ($OR = 1.03$). Notably, gender, race and employment status appear to not affect whether one adopts SPBs or not.

Discussion

The review of the literature revealed a gap in our understanding of the mechanisms of adoption of SPBs to prevent repeat victimisation against cyber abuse. Aiming to address this gap, this study had a dual focus: 1) to

Table 3 Logistic regression with Bayesian variable selection explaining the adoption of SPBs following cyber abuse victimisation accounting for the method of abuse experienced by the victim ($N = 746$). Check marks denote coefficients included in the models

Coefficient	β	SD	2.5% HPD[b]	97.5% HPD[b]	Pr($\beta \neq 0$) %[c]	Model[a] 1	2	3	4	5
Constant	− 2.85	0.45	− 3.77	− 1.98	100	✓	✓	✓	✓	✓
Method 5	1.11	0.21	0.69	1.52	100	✓	✓	✓	✓	✓
Impact	1.57	0.18	1.21	1.92	100	✓	✓	✓	✓	✓
OVR	− 0.81	0.23	− 1.24	− 0.38	99	✓	✓	✓	✓	
Age	0.03	0.01	0.01	0.05	94	✓	✓	✓	✓	✓
Method 4	0.18	0.27	0.00	0.77	39		✓		✓	
Gender	0.09	0.17	0.00	0.51	29			✓	✓	
Method 1	0.04	0.12	0.00	0.39	17					✓
Method 3	− 0.02	0.09	− 0.30	0.04	12					
Employment	0.01	0.08	− 0.04	0.21	9					
Method 2	− 0.01	0.07	− 0.22	0.00	9					
Race	− 0.01	0.06	− 0.18	0.02	8					
Posterior Probability of the model (%)						24.3	13.2	9.1	6.7	4.9

[a] Best 5 models (cumulative posterior probability = 59.1%)

[b] Highest Posterior Density

[c] Probability of inclusion

Table 4 Reflective journal example entry

Question	*Example entry*
1. What triggered the SPB?	Break up of a romantic relationship.
2. What did the abuse entail?	The victim was sent a large number of threatening and insulting messages via her social media account.
3. What did the victim do to prevent repeat victimisation	The victim has blocked the abuser in social media.
4. Any additional steps the victim undertook as a precaution?	The victim also adjusted her social media account's privacy settings to be visible to friends only.
5. What did the victim try to accomplish?	The goal was to block the abuser from accessing the victim.
6. How was this goal accomplished?	By reducing the accessibility of the victim and reducing the visibility of the victim's social media account.

establish a typology of SPBs to prevent repeat victimisation from cyber abuse, and 2) to learn more about victims of cyber abuse who adopt SPBs to prevent repeat victimisation.

Our findings suggest that a large proportion (around 40%) of victims of cyber abuse adopted at least one type of SPB following the initial incident, and many adopted multiple SPBs. This suggests that while on average, cyber abuse is often not serious enough to warrant preventive action, in some circumstances and for some victims it is. Our study focused only on changes in behaviour in relation to the use of technology, so with this in mind we identified only six different types of SPBs victims use to prevent cyber abuse, including (1) adjusting privacy settings, (2) blocking abusive contacts, (3) improving security, (4) self-censorship, (5) avoiding sharing private information, and finally, (6) avoiding technology/social media altogether. We found that adjusting privacy settings was the most popular and improving security was the least popular SPB with the victims in our sample. These findings are not dissimilar to the previous literature, in particular, the study by Tokunaga and Aune (2017). Future research using a large probability-based sample should provide further evidence needed to develop a comprehensive typology of SPBs in the context of technology-generated crime and deviance.

Our study was able to provide some new insights into the factors associated with the adoption of SPBs to prevent repeat victimisation from cyber abuse. Using our data, being older, significantly affected by the event and

abused by a stranger are significant predictors of SPBs. In line with previous literature, we found that seriousness of victimisation, operationalised in our study as victim impact and number of methods of abuse experienced by the victim, is an important factor predictive of the adoption of SPBs. This finding further supports the rational choice perspective's assumption that victims engage in cost-benefit analysis when deciding "to SPB or not to SPB" and that the adoption of SPBs is more likely when the anticipated cost of repeat victimisation is significant. Also, in line with the rational choice's ideas of cost-benefit analysis, we found that SPBs that appear to be less costly in terms of the required effort and the associated loss of utility are more popular than the costlier types. In particular, we found that a fairly straightforward SPB of adjusting privacy settings is a more common SPB than for example, fully disengaging from the online discourse by avoiding the use of technology.

Interestingly, the type of method of abuse experienced by the victim was also found to be predictive of SPBs. Our findings suggest that victims who experienced surveillance of their online activities and to a lesser degree, someone impersonating them online to be much more likely to act to prevent repeat victimisation than the victims of all other examined methods of abuse. This is an important finding as previous research mostly compared SPBs adopted by victims of offline and online forms of stalking and did not examine the effect of specific types of abuse of the likelihood of adopting SPBs. Our study provides the first evidence that variation of deviance type within one crime category (i.e. cyber abuse) is an important factor that determines whether a victim is likely to adopt an SPB or not. We suspect this effect is explained by the intrinsic characteristics of the specific method of abuse that make it somehow more or less unbearable and is probably at least somewhat related to the seriousness of the abuse. Significant positive (albeit quite weak) correlations between victims impact and Method 4 (online impersonation) and Method 5 (surveillance) (see Table 2 seem to support this suggestion. It is possible that being monitored may be particularly unpleasant due to the uncertain and potentially more dangerous consequences. It is, however, possible that the reason for this finding is in the ease of implementation of SPBs designed to prevent these specific methods of abuse. For example, it may be easier to prevent your online activities being followed by managing your privacy settings on social media, however, it may be much more difficult to preclude someone from posting your personal information (e.g. nude photos) online where external social control or law enforcement entities may have to be involved.[9] Further investigation of this finding is warranted.

Limitations

Our findings should be interpreted in light of the limitations of this study. First, considering the non-probability nature of our sample, we cannot generalize the findings to our target population (i.e. adult U.S. residents). Second, the data analysed in this study is based on self-reports of victims of cyber abuse and may suffer from several potential biases, recall issues and other issues common for this type of data. We note however that compared with traditional methods of data collection, such as face-to-face or phone interviews, online surveys are associated with reduced interviewer-induced measurement errors and social desirability bias (Baker et al. 2010; Chang and Krosnick 2009; Kreuter et al. 2008; Sue and Ritter 2012). Third, the cross-sectional nature of the design of this study means that we could not establish whether the adoption of self-protective behaviours influences the risk of re-victimization. Fourth, while a clear improvement on previous research that focused on developing a typology of SPBs in cyberspace in terms of the sample size and the diversity of respondents included in the sample (research by Tokunaga and Aune (2017), for example, employed a small sample of only 51 subjects drawn from university students and Facebook participants), the non-probability nature of our sample means that some SPBs used by the individuals that are underrepresented (for example, non-whites) or possibly not represented at all in our sample may be missing from our findings. And finally, using our research design, we cannot tell whether the reason why some methods of cyber abuse are associated with higher rates of adoption of SPBs than others is due to the ease of implementing or availability of appropriate SPBs. With previous research mostly focusing on the benefit of preventing repeat victimisation part of the rational choice-based explanatory model of the adoption of SPBs, estimating the effect of ease of implementation and/or availability of different types of SPBs would significantly improve the overall by adding *the cost of preventive action* part of the equation.

Conclusion

In conclusion, this study examined an under-researched issue, the adoption of self-protective behaviours by victims of cyber abuse to prevent repeat victimisation. Using a mixed-method approach, it focused on improving our knowledge about who adopts SPBs, what kind and under

[9] The authors would like to thank the anonymous reviewer for suggesting this possible explanation.

what circumstances. This study contributes to the overall knowledge base in two ways. First, we proposed a new typology of self-protective behaviours adopted by victims of cyber abuse to prevent repeat victimisation from cyber abuse. And second, we identified several factors, mainly in line with previous research, that are important predictors of self-protective behaviours in the context of technology-driven deviance. The findings from this study have direct practical application for developing crime prevention strategies against cyber abuse and would be useful for anyone involved in providing advice to victims, including support centres and law enforcement. Our findings could be used to educate victims about the types of SPBs available to them to prevent repeat victimisation.

This study could be extended in several potentially fruitful directions. First, as the data are cross-sectional, we could not establish whether the adoption of SPBs actually influences the risk of repeat victimisation. Future research utilising an experimental or longitudinal design should examine the effectiveness of SPBs against repeat victimisation from cyber abuse. It would also be interesting to compare different SPBs in terms of their effectiveness or otherwise. And second, while it is clear from our findings that some SPBs are more popular than others, it is not clear what part of their popularity is explained by the availability of particular technological tools vs. ease of use. This is particularly relevant to SPBs involving things like privacy maintenance, improving security, etc. Future research should examine the SPBs' ease of use/availability dichotomy. The findings would be critical to the development of new social media software that makes it easy for its user to self-protect.

Acknowledgements
The authors would like to thank Professor Henk Elffers and Professor Ken Pease for their critical feedback on the earlier drafts of the paper.

Authors' contributions
ZIV, CAS, CLA and RIM designed the study, ZIV collected the data, CAS coded and analysed textual data, ZIV and CAS coded and analysed numerical data, ZIV, CAS, CLA and RIM authored the article. All authors read and approved the final manuscript.

Funding
No outside funding was used to support this work.

Availability of data and materials
Variance-co-variance matrix and detailed descriptive statistics may be requested from Dr Zarina Vakhitova at Zarina@Vakhitova.com.

Competing interests
The authors declare that they have no competing interests.

Author details
[1] Monash University, Clayton Campus, Menzies Building, 20 Chancellors Walk, Victoria 3800, Australia. [2] Harper Adams University, Edgmond, Newport TF10 8NB, United Kingdom. [3] Predictive Analytics Group, Level 7 South, 175 Collins Street, Melbourne, Vic 3000, Australia.

Appendix A

Received: 19 April 2020 Accepted: 30 October 2020
Published online: 11 November 2020

References

Akers, C., & Kaukinen, C. (2009). The police reporting behavior of intimate partner violence victims. *Journal of Family Violence,24*, 159–171.
Ando, T. (2010). *Bayesian model selection and statistical modeling*. New-York: CRC.
Averdijk, M. (2011). Reciprocal effects of victimization and routine activities. *Journal of Quantitative Criminology,27*(2), 125–149. https://doi.org/10.1007/s10940-010-9106-6.
Baker, R., Blumberg, S., Brick, J., Couper, M., Courtright, M., Dennis, J., et al. (2010). Research synthesis: AAPOR report on online panels. *Public Opinion Quarterly,74*, 711–781.
Baum, K., Catalano, S., Rand, M., & Rose, K. (2009). *Stalking victimisation in the United States*. Washington, D.C: Bureau of Justice Statistics.
Beccaria, C. (1764). On crimes and punishments H. Paolucci, Trans., 1963. New York: Pearson Education.
Becker, G.S. (1976). The economic approach to human behavior. University of Chicago Press. Retrieved from https://books.google.com.au/books?id=qQAZnc-mMSoC.
Behrend, T., Sharek, D., Meade, A., & Wiebe, E. (2011). The viability of crowdsourcing for survey research. *Behavior Research Methods,43*, 800–813.
Bentham, J. (1789). The principles of morals and legislation. Amherst: Prometheus Books.
Bocij, P. (2006). *Cyberstalking: Harassment in the internet age and how to protect your family*. Westpoint, CT: Praeger Publishers.
Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology,3*, 77–101.
Browning, G., Halcli, A., & Webster, F. (2000). *Understanding Contemporary Society: Theories of the Present*. London: SAGE Publications.
Buhi, E., Clayton, H., & Surrency, H. (2009). Stalking victimization among college women and subsequent help-seeking behavior. *Journal of American College Health,57*, 419–425.
Bunch, J., Clay-Warner, J., & McMahon-Howard, J. (2014). The effects of victimization on routine activities. *Criminal Justice and Behaviour,41*, 574–592.
Chang, L. C., & Krosnick, J. (2009). National surveys via RDD telephone interviewing versus the Internet: Comparing sample representativeness and response quality. *Public Opinion Quarterly,73*, 641–678.
Clarke, R.V., & Cornish, D.B. (1985). Modeling offenders' decisions: A framework for research and policy. In: Crime and justice (vol. 6). Chicago: University of Chicago Press.
Cornish, D. B., & Clarke, R. V. (1986). *Introduction The reasoning criminal* (Vol. 6, pp. 2–16). New York: Springer.
Denver, M., Pickett, J. T., & Bushway, S. D. (2018). Criminal records and employment: A survey of experiences and attitudes in the United States. *Justice Quarterly,35*, 584–613.
Dreßing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behaviours and Social Networking,17*, 61–67.
Duggan, M. (2017). Online harassment. Retrieved from http://www.pewinternet.org/2017/07/11/online-harassment-2017/.
Enns, P. K., & Ramirez, M. (2018). Privatizing punishment: Testing theories of public support for private prison and immigration detention facilities. *Criminology,56*, 546–573.
Finkelhor, D., & Asdigian, N. (1996). Risk factors for youth victimization: Beyond a lifestyle-routine activities theory approach. *Violence and Victims,11*, 3–19.
Fisher, B., Daigle, L., Cullen, F., & Turner, M. (2003). Reporting sexual victimization to the police and others. *Criminal Justice and Behavior,30*, 6–38. https://doi.org/10.1177/0093854802239161.
Fissel, E. (2018). The reporting and help-seeking behaviours of cyberstalking victims. *Journal of Interpersonal Violence, 24*, 1–26.

Gottfredson, M. R., & Gottfredson, D. M. (1988). *Decision making in criminal justice: Toward the rational exercise of discretion* (2nd ed.). New York, NY: Plenum.
Gottfredson, M. R., & Hindelang, M. J. (1979). A study of behaviour of law. *American Sociological Review,44*, 3–18.
Gottlieb, A. (2017). The effect of message frames on public attitudes toward criminal justice reform for nonviolent offenses. *Crime and Delinquency, 63*, 636–656.
Groenendyk, E. (2016). The anxious and ambivalent partisan: The effect of incidental anxiety on partisan motivated recall and ambivalence. *Public Opinion Quarterly,80*, 460–479.
Guerette, R., & Santana, S. (2010). Explaining victim self-protective behaviour effects on crime incident outcomes: A test of opportunity theory. *Crime & Delinquency,56*, 198–226.
Hampton, K., Rainie, L., Lu, W., Dwyer, M., Shin, I., & Purcell, K. (2014). Social media and the "Spiral of Silence". Pew Research Center. https://www.pewresearch.org/internet/2014/08/26/social-media-and-the-spiral-of-silence/. Retrived from 12 Dec 2019.
Hayes, A., Glynn, G., & Shanahan, J. (2005). Validating the willingness to self-censor scale: Individual differences in the effect of the climate of opinion on opinion expression. *International Journal of Public Opinion Research,7*, 443–455.
Herath, T., & Rao, R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *Ejis,18*, 106–125. https://doi.org/10.1057/ejis.2009.6.
Hoeting, J.A., Madigan, D., Raftery, A.E., & Volinsky, C. (1999). Bayesian model averaging: A tutorial. Statistical Science, 14, 4, 382–401. Retrieved from http://www.jstor.org/stable/2676803.
Hokoda, A., Hsuch-Huei, L., & Angeles, M. (2006). School bullying in taiwanese adolescents. *Journal of Emotional Abuse,6*, 69–90.
Kreuter, F., Presser, S., & Tourangeau, R. (2008). Social desirability bias in CATI, IVR, and Web surveys: The effects of mode and question sensitivity. *Public Opinion Quarterly,72*, 847–865.
Krippendorff, K. (2013). *Content analysis: An introduction to its methodology* (3rd ed.). Thousand Oaks, CA: Sage.
Loughran, T. A., Paternoster, R., Chalfin, A., & Wilson, T. (2016). Can rational choice be considered a general theory of crime? Evidence from individual-level panel data. *Criminology, 54*(1), 86–112. https://doi.org/10.1111/1745-9125.12097.
Loughran, T. A., Paternoster, R., Piquero, A. R., & Pogarsky, G. (2011). On ambiguity in perceptions of risk: Implications for criminal decision making and deterrence. *Criminology, 49*(4), 1029–1061. https://doi.org/10.1111/j.1745-9125.2011.00251.x.
Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9.
Madigan, D., & Raftery, A. E. (1994). Model selection and accounting for model uncertainty in graphical models using Occam's window. *Journal of the American Statistical Association,89*, 1535–1546.
Marin, J. M., & Robert, C. P. (2014). *Bayesian essentials with R*. New York: Springer.
McCarthy, B., & Chaudhary, A. (2014). Rational choice theory. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. 4307–4315). New York: Springer.
Melander, L. A. (2010). College students' perceptions of intimate partner cyber harassment. *Cyberpsychology, Behavior, and Social Networking,13*, 263–268. https://doi.org/10.1007/s10940-010-9106-6.
Nobles, M., Reyns, B., Fox, K., & Fisher, B. (2014). Protection against pursuit: A conceptual and empirical comparison of cyberstalking an stalking victimization among a national sample. *Justice Quarterly,31*, 986–1014.
Noelle-Neumann, E. (2006). The spiral of silence a theory of public opinion. *Journal of Communication,24*(2), 43–51. https://doi.org/10.1007/s10940-010-9106-6.
Pereira, F., Spitzberg, B. H., & Matos, M. (2016). Cyber-harassment victimization in portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior, 62*, 136–146. https://doi.org/10.1016/j.chb.2016.03.039.
Phillips, F., & Morrisey, G. (2004). Cyberstalking and cyberpredators: A threat to safe sexuality on the internet. *Convergence,10*, 66–79.
Pickett, J. T., Barnes, J. C., Wilson, T., & Roche, S. P. (2019). Prospect theory and criminal choice: Experiments testing framing, reference dependence, and decision weights. *Justice Quarterly, 98*, 1–29. https://doi.org/10.1080/07418825.2018.1531142.
Pickett, J. T., & Bushway, S. D. (2015). Dispositional sources of sanction perceptions: Emotionality, cognitive style, intolerance of ambiguity, and self-efficacy. *Law and Human Behavior,39*(6), 624–640.
Pickett, J. T., Roche, S. P., & Pogarsky, G. (2018). Toward a bifurcated theory of emotional deterrence. *Criminology,56*(1), 27–58. https://doi.org/10.1007/s10940-010-9106-6.
Raftery, A. (1995). Bayesian model selection in social research. *Sociological Methodology,25*, 111–163.
Reyns, B. W., & Englebrecht, C. M. (2010). The stalking victim's decision to contact the police: A test of Gottfredson and Gottfredson's theory of criminal justice decision making. *Journal of Criminal Justice,38*(5), 998–1005. https://doi.org/10.1007/s10940-010-9106-6.
Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology,91*(1), 93–114. https://doi.org/10.1007/s10940-010-9106-6.
Sheridan, L., & Grant, T. (2007). *Is cyberstalking different?* (p. 13). Crime & Law: Psychology.
Short, E., Guppy, A., Hart, J., & Barnes, J. (2015). The impact of cyberstalking. *Studies in Media and Communications, 3*, 1–15.
Short, E., Linford, S., Wheatford, J., & Maple, C. (2014). The impact of stalking: The lived experience—a thematic analysis. *Studies in Health Technology and Informatics,199*, 133–137.
Skogan, W. G. (1981). *On attitudes and behaviours*. Beverly Hills: Sage Publications.
Statistics Canada. (2016). Study: Cyberbullying and cyberstalking among Internet users aged 15 to 29 in Canada. Retrived from http://www.statcan.gc.ca/daily-quotidien/161219/dq161219a-eng.htm?HPA=1. 08 Aug 2020.
Sue, V., & Ritter, L. (2012). *Conducting online surveys*. Thousand Oaks, CA: Sage.
Thompson, R., Tseloni, A., Tilley, N., Farrell, G., & Pease, K. (2018). Which security devices reduce burglary? In A. Tseloni, R. Thompson, & N. Tilley (Eds.), *Reducing burglary*. Cham: Springer.
Tokunaga, R. S., & Aune, K. S. (2017). Cyber-defense: A taxonomy of tactics for managing cyberstalking. *Journal of Interpersonal Violence,32*(10), 1451–1475.
Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009.
Vakhitova, Z. I., & Alston-Knox, C. L. (2018). Non-significant p-values? Strategies to understand and better determine the importance of effects and interactions in logistic regression. *PLoS ONE,13*, 11. https://doi.org/10.1007/s10940-010-9106-6.
Vakhitova, Z.I. , Alston-Knox, C.L., Mawby, R.I. & Reeves, E. (in press). Explaining victim impact from cyber abuse: An exploratory mixed methods analysis. Deviant behaviour.
Vakhitova, Z. I., Alston-Knox, C. L., Webster, J. L., Reynald, D. M., & Townsley, M. K. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse? *Computers in Human Behaviour,101*, 225–237. https://books.google.com.au/books?id=qQAZnc-mMSoC0.
Vakhitova, Z. I., & Reynald, D. M. (2014). Australian internet users and guardianship against cyber abuse: An empirical analysis. *International Journal of Cyber Criminology,8*, 156–171.
Vakhitova, Z. I., Reynald, D. M., & Townsley, M. K. (2016). Toward adapting routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice,32*(2), 169–188.
Vakhitova, Z. I., Webster, J. L., Alston-Knox, C. L., Reynald, D. M., & Towsnley, M. K. (2018). Offender-victim relationship and offender motivation in the context of indirect cyber abuse: A mixed-method exploratory analysis. *International Review of Victimology,24*(3), 347–366. https://books.google.com.au/books?id=qQAZnc-mMSoC.
Vaughan, T. J., Holleran, L. B., & Silver, J. (2019). Applying moral foundations theory to the explanation of capital jurors' sentencing decisions. *Justice Quarterly*. https://doi.org/10.1080/07418825.2018.1537400.
Weisel, D.L. (2005). Analyzing repeat victimization. (vol. 4). U.S. Department of Justice. Office of Community Oriented Policing Services. Retrieved from https://books.google.com.au/books?id=qQAZnc-mMSoC.
Wilcox, P., Jordan, C., & Pritchard, A. (2007). A multidimensional examination of campus safety: Victimization, perceptions of danger, worry about crime,

and precautionary behavior among college women in the post-Clery era. *Crime & Delinquency,53*, 219–254.
Williams, S. D. (2002). Self-esteem and the self-censorship of creative ideas. *Personnel Review,31*, 495–503.
Wong, D. S., Chan, H. C. O., & Cheng, C. H. (2014). Cyberbullying perpetration and victimization among adolescents in hong kong. *Children and Youth Services Review,36*, 133–140. https://books.google.com.au/books?id=qQAZnc-mMSoC.
Worsley, J., Wheatcroft, J., Short, E., & Corcoran, R. (2016). Victim's voices: Understanding the emotional impact of cyberstalking and individual's coping responses. *SAGE Open,7*, 1–13.
Wortley, R., & Sidebottom, A. (2017). Deterrence and rational choice theory. In: The encyclopedia of juvenile delinquency and justice (pp. 1–6). American Cancer Society. https://doi.org/10.1002/9781118524275.ejdj0131.
Wykes, M. (2007). Constructing crime: Culture, stalking, celebrity and cyber. *Crime, Media, Culture, 3*, 158–174.

Publisher's Note