Article

Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship

Jelle Brands
Leiden University, The Netherlands

Johan van Wilsem
Netherlands Court of Audit, The Netherlands

Abstract

Although it is generally acknowledged that the development of the Internet created new criminal opportunities, the ways this is experienced by the general population has received limited attention. The current study seeks to explore the degrees to which people report fear of online crime, its correlates, and how online fear is related to protective and avoidance behaviour. We focus on online financial crimes. Results based on a large, representative, survey indicate an intermediate level of fear of online crime among the general Dutch population. Various sociodemographic characteristics and victimization experiences are shown to predict fear of online financial crime. We also find online fear to be a strong predictor of avoidance behaviour, given negative relationships with online purchasing and banking, thereby impeding individuals' perceived online freedom and opportunities. Finally, the results found no indications that fear may stimulate protective behaviour of one's computer.

Keywords

Corresponding author:
Jelle Brands, Department of Criminology, Leiden University, Steenschuur 25, Leiden, 2311 ES, The Netherlands.
Email: j.brands@law.leidenuniv.nl

Introduction

The advance of the Internet has greatly influenced the way we go about our everyday lives: it has transformed the ways we do 'business, work, consumption, leisure and politics' (Yar, 2013: 4). Many such developments can be placed in a positive sphere, augmenting the agency of individuals and expanding their freedoms and liberties (Yar, 2009), or in terms of potential drivers for economic growth (Virtanen, 2017). Yet, more pessimistic views about the advance of the Internet have also found a foothold in society. Of particular interest here, the 'Internet brings with it new threats and dangers to our well-being and security' (Yar, 2013: 4).[1] Alongside this development, a fruitful field of studies has emerged in criminology looking into the identification and quantification of these 'new threats and dangers' brought about by the Internet, their dimensions, as well as online offenders (Brenner, 2014; Holt and Bossler, 2014). In addition, the victimology literature has drawn attention to online victimization and victims (Holt and Bossler, 2008; Leukfeldt, 2015; Ngo and Paternoster, 2011; Reyns, 2015; Van Wilsem, 2011, 2013). But less headway has been made in studying how these 'new threats and dangers' are experienced by the general population (Henson and Reyns, 2015; Jansen et al., 2017).

It is noteworthy that only a limited number of empirical studies are available on the ways in which online threats and dangers are experienced by the general public. After all, the subjective dimensions of victimization – especially in terms of fear of criminal victimization – have received substantial attention in the criminological literature more generally (see, for instance, Farrall et al., 2012; Hale, 1996; Henson and Reyns, 2015; Lee and Mythen, 2018; Spithoven, 2017). Indeed, outlining the evolution of the fear of crime literature, Henson and Reyns (2015: 94) argue that '[t]o date, only a handful of studies have focused on fear of online victimization. As online victimization has become an emerging area of research, more research into fear of online victimization is warranted.'

To be sure, however, there are a growing number of studies preoccupied with fear of online crime (see below). Reviewing the available studies, a number of limitations are nonetheless apparent. First, the research base on the topic seems fairly fragmented. One reason for this is that the 'object' of fear differs substantially between studies, from fairly specific worries about a particular online crime to measures merging a variety of online crimes into a general 'fear of crime' variable. Another is that studies use inconsistent measures of fear. As Hinkle (2015: 148) points out, our understanding of fear of crime is muddied when researchers confuse other constructs with fear of crime and/or when 'concepts are erroneously labelled "fear of crime"'. Also, individual studies tend to single out specific (key) predictors to explain fear of online crime. One result is that it is not sufficiently clear if/how such predictors are related to fear of particular types of online crime. Second, studies drawing on a larger and representative sample of the general population are scarce (but see Reisig et al., 2009; Roberts et al., 2013), especially for the European context (but see European Commission, 2017; Virtanen, 2017). Third, although it is well documented in the literature that fear of crime can and does affect behaviour (Doran and Burgess, 2012; Lorenc et al., 2012; Liska et al., 1988; Rader, 2004; Rader et al., 2007; Warr, 2000), these links have received scant attention in studies focusing on online contexts. It is nonetheless important to better understand behavioural responses as a result of fear of crime, because these may have unwelcome effects at the personal level (unequal

access through avoidance, and increased spending on protective measures)[2] but also have undesirable economic consequences for society at large: they may drive consumer spending away from amenities (Doran and Burgess, 2012; Hille et al., 2015).

The current study, then, aims to explain both which people experience online worries and fears, and subsequently the ways these fears are linked to online behaviours. We specifically focus our research efforts on fear of online financial crime. We motivate this focus by pointing out that a broad variety of online behaviours are related to running the risk of suffering online financial crimes. For instance, by clicking links on mala fide online advertisements users' computers may become infected with malware, which opens opportunities for committing financial crimes (Van Wegberg et al., 2017). The same holds for supposed communication with one's bank, which may actually be a phishing attempt, or online purchases in which the provision of client information to complete the transaction is either not safely transmitted or stored by the online shop. As a consequence, victimization experiences related to an online financial crime or a preparatory stage of that (hacking, malware infection) make up a large share of the total number of cybercrime victimization experiences. In an effort to prevent these crimes from happening to them – and possibly as an outcome of fear of these crimes – people may avoid certain online situations or apply protective measures. Fear of online financial crime may therefore have the potential to impede a variety of regular online behaviours, including online banking and online shopping, on which the current study focuses.

In order to study fear of online financial crime and the ways this relates to online behaviour, we draw on the data of a large, representative survey distributed among the Dutch general population. In so doing, it is important to note in advance that the Dutch, as compared with the EU average, should be considered frequent users of (the) Internet (services). Recent statistics by Eurostat (2018) indicate that the Dutch enjoy the highest Internet access (98 percent) among the EU countries (87 percent average). And, according to the European Commission Special Eurobarometer 431 report (European Commission, 2015), 75 percent of the Dutch use online banking every week, whereas the EU average is 43 percent. Only 9 percent of the Dutch have never used online banking (EU average 35 percent). The Dutch, however, tend to buy slightly fewer goods and services online on a weekly basis (15 percent) compared with the EU average (17 percent). In turn, 12 percent of the Dutch have never bought goods or services online, whereas this is 24 percent for the EU as a whole.

Fear of online crime

Measurement and conceptualization: Lessons learned from the fear of crime literature

From the 1960s onwards, fear of crime has emerged as, and remained, a pressing issue on the policy agenda (Farrall et al., 2012; Henson and Reyns, 2015). At least part of the consequent academic discussion focused on the measurement and conceptualization of fear of crime. Even if we are here specifically interested in the fear of online crime, an overview of the progress made in the fear of crime studies literature is also relevant in light of the current study.[3] Much can be learned from the existing research base, and important principles should also be heeded when studying fear of online crime.

To start with, there is by now some agreement among scholars that 'fear of crime involves feelings, thoughts, and behaviours, all of which are focused on the subjectively conceived threat of criminal victimization' (Jackson and Gouseti, 2013: 2). In other words, the fear of crime includes emotive/affective, cognitive and behavioural dimensions (see also Ferraro and LaGrange, 1987; Rader, 2004; Rader et al., 2007; Spithoven, 2017). Early studies into the fear of crime were often criticized in terms of their inability to differentiate between these dimensions. One reason for this was the widespread use of 'perceived safety measures', and more specifically the frequent use of a standard question to study fear of crime: 'How safe do you feel or would you feel being out alone in your neighbourhood at night' (Hinkle, 2015: 150). According to Farrall et al. (2012: 48), one limitation of 'perceived safety measures' is that they 'conflate measures of "fear" with measures of judgements of threat'. Whereas the two are related, they should not be considered to measure the same thing (Farrall et al., 2012; Farrall and Gadd, 2004; Fattah, 1993; Warr, 2000). Risk perceptions are about people's cognitive assessments of personal risk, their perceptions of the likelihood of falling victim to criminal victimization. The affective/emotive dimension of fear of crime, on the other hand, can be understood in terms of a range of emotions related to the possibility of criminal victimization. These include fear, worry and (widespread but diffuse) anxiety (Jackson and Gouseti, 2013) about crime; see Jackson and Gouseti (2013: 2) for a useful distinction between the three). Following these critiques, (survey) questions designed to measure emotion, related to the possibility of criminal victimization, have been refined over time. It is by now generally acknowledged good practice that questions tapping into this aspect of fear of crime should refer to emotion (for instance, 'how afraid'), specifically mention (a) crime, and refer to realistic scenarios (Ferraro and LaGrange, 1987; Gray et al., 2012; Hinkle, 2015; Warr, 2000).

Fear of crime scholars have also started to distinguish between intensity measures of fear of crime and what could be referred to as situated or frequency measures of fear of crime. Accordingly, whereas the fear of crime is most regularly approached making use of intensity measures that ask for some sort of general summary about the intensity of respondents' feelings (very worried/fearful – not worried/fearful at all about this or that), according to Jackson (2005: 299) a consequence of approaching fear of crime like this is that 'intensity measures have encouraged the idea that fear is a stable attribute rather than something that varies across time, location and situations'. In terms of measurement, this means that we can measure fear of (online) crime in terms of 'concrete moments of fear (which can be measured in terms of frequency) and[/or] a more diffuse but emotionally tinged anxiety about crime (which is invoked by standard questions; e.g., How worried are you…?)' (Gray et al., 2012: 13).

Finally, studies also point out a behavioural dimension to the fear of crime and generally consider fear and behaviour to be associated with one another (Rader, 2004; Rader et al., 2007). Indeed, Warr (2000: 459) argues that '[n]early all those who have investigated the emotion of fear agree that fear reveals itself through behaviour'. This is also empirically substantiated by Liska et al. (1988), who applied a reciprocal effects model to their (National Crime Survey) data in order to untangle the temporal ordering of effects. They concluded that 'fear and constrained social behaviour are part of a positive escalating loop (fear constrains social behaviour which increases fear)' (p. 827). The

literature also suggests that the behavioural dimension to fear of crime may be broken down into the sub-dimensions of protective behaviours and avoidance behaviours (Liska et al., 1988). Avoidance behaviours refer to the actions people take to minimize contact with criminal environments as a result of feeling threatened by crime. Examples in the literature include avoiding particular areas in the city, such as deprived neighbourhoods or urban parks, especially at night. In terms of online environments, we might think of avoiding particular online services and/or websites. Protective behaviours, on the other hand, are measures taken to resist or deter crime (Jackson and Gouseti, 2013). Among other things, taking self-defence classes, carrying around objects such as pepper spray, but also home security measures are mentioned in the literature (Reid et al., 1998; Spithoven, 2017; Starkweather, 2007). For the online environment, we might think of the application of protective measures such as installing a firewall or a virus scanner.

What follows from the above, then, is that it is critically important for research into fear of (online) crime to be specific about, and to conceptually differentiate between, what it seeks to measure. The current study will focus on the affective dimension of the fear of crime, and it approaches fear of online crime by making use of intensity measures. From the review above, it can also be hypothesized that a positive relationship exists between fear of online crime and online avoidance behaviours and protective behaviours on one's personal computer.

Below we provide a review of available studies that have previously investigated fears of online crimes using intensity measures. In doing so, we draw specific attention to studies investigating fears and worries about financial crimes in online environments and the central theoretical mechanisms that have been proffered to explain it. A final step in our review of the literature consists of scrutinizing the evidence base on the (theoretical) links between fear of online crime and online avoidance and protective behaviours.

Fears and worries about online financial crime, victimization and vulnerabilities

In the fear of crime literature, victimization experience is proposed as one of the earliest predictors. This variable has since been studied at both the individual and the neighbourhood level, delivering mixed results (Farrall et al., 2012). Alternatively, the imagined victimization model posits that fear of and worry about crime are linked to what people indirectly hear about crime victimization, providing a lens through which they may imagine themselves falling victim to crime and becoming fearful (Farrall et al., 2012; Jansen et al., 2017). According to Farrall et al. (2012), perceptions of victimization are also linked to vulnerabilities, which in turn may explain differences in fear of crime between groups of individuals (Ferraro and LaGrange, 1987). As a means to model the effects of vulnerabilities on fear of crime, studies often use proxies such as age, gender, ethnicity and socioeconomic status (but see Jackson, 2009, for a more detailed approach). Socioeconomic status and ethnicity are often considered to be indicators of socioeconomic vulnerability. Because people with a lower social position are considered to have fewer resources to prevent, and cope with, the consequences of victimization, they may experience greater vulnerability (Spithoven, 2017). It can reasonably be hypothesized

that this mechanism applies to both offline and online environments. Gender and age are often positioned as indicators of physical vulnerability, which involves an individual's perception of the capacity to effectively (physically) defend oneself. Theorizing gender and age through the lens of physical vulnerability might be less relevant here, however, taking into consideration the non-physical nature of the crime under study. At the same time, Jackson and Gouseti (2013: 3) argue that, 'since vulnerability is stereotypically compatible with traditional notions of femininity', this means that answers to questions about fear of crime may function as a means to express identity and gendered norms, and as such differ in intensity between males and females. This means that gender may also be linked to social vulnerability 'as a product of more sensitive [gender] socialisation' (Spithoven, 2017: 26). Possibly, such a mechanism also extends to the role of age in producing fear of online crime. What is more, Virtanen (2017: 325) approaches the confidence people have in their abilities to use the Internet as another type of social vulnerability. It could be hypothesized that older age may be related to greater worries about online crimes through the confidence people have in their abilities to use the Internet, since there is some evidence that older people experience greater computer anxiety, defined in Powell (2013) as a feeling of unease or apprehension about current (or future) use of computers.

Studies accounting for the effects of previous victimization on fear of financial crime in online environments report mixed results. Virtanen (2017: 330) reports that 'all types of prior experience with online crime (harassment, hacking, fraud, cyberattacks) predict general fear of cybercrime'. It should be taken into account, however, that the dependent variable 'fear of cybercrime' in this study is constructed from a range of items including, but not restricted to, questions about online financial crimes. In contrast to this result, no significant relationship between victimization and fear of online crime is reported by Jansen et al. (2017), who include various items that ask about online financial crimes as part of a broader measure. Neither does victimization experience reach significance in Yu (2014), who studied fear of being scammed.

Studies investigating fear of online financial crime also include socioeconomic vulnerability in their models. Results in Virtanen (2017) indicate that (self-reported) social status is statistically significantly related to fear of online crime. Ethnicity does not reach statistical significance in Yu (2014). Jansen et al. (2017) report a significant, negative, effect for education. Roberts et al. (2013) – who studied fear of cyber-identity theft and related fraudulent activity – also included education in their analysis, but find no significant results in their final, most extensive, model. With regards to age, available studies report mixed results. In Roberts et al. (2013), older participants significantly express greater fear. Virtanen (2017), however, reports a significant effect in the opposite direction. Jansen et al. (2017) also find a significant, negative effect for age. Yu (2014), on the other hand, reports no significant result for age. Finally, we find that gender is included in most studies investigating fear of online financial crime. In Virtanen (2017), women reported significantly higher fear, as did women in Jansen et al. (2017). Roberts et al. (2013) and Yu (2014), on the other hand, report no significant relationship between gender and fear of online crime. It should, however (and again), be noted that in Virtanen (2017) and Jansen et al. (2017) more general measures of fear of online crime are reported, possibly explaining the differences in these results.

Fears and worries about online financial crime and online protective and avoidance behaviour

Building on the fear of crime literature, we hypothesize that, apart from being a consequence (for example of vulnerability and/or victimization, above), fear of online crime can also function and be studied as a cause of online avoidance and protective behaviours. As we saw above, this link between fear of crime and behaviour pertains to a first step of a positive escalating loop as presented by Liska et al. (1988). In the current study, we specifically focus on online banking and purchasing behaviour (which people may avoid, or not), as well as the application of protective measures on one's computer.

There are some studies available that have investigated fear of online crime in relation to online banking and/or shopping. A study by Böhme and Moore (2012) indicates that EU citizens who express more concern, either general or personal, over cybercrime report lower online participation, specified as buying online and banking online. Importantly, however, they mention that they 'consider fear of crime to be implicitly included [part of their risk measure], assuming that emotional reactions also influence how people react to cybercrime' (Riek et al., 2016: 3). Similarly, Forsythe and Shi (2003) and Reisig et al. (2009) find empirical support for the relationship between perceived online risk and purchasing online and spending time online among, respectively, 'Internet users who have access to the World Wide Web' and 'Internet users in the state of Florida'. But perhaps most convincing on the matter is the study by Hille et al. (2015: 13) reporting a significant negative relationship between fear of financial losses related to online identity theft and online purchase intention among members of a major music label's online costumer panel. A study coupling online fears/worries to actual, revealed, behaviour is nonetheless lacking to our current knowledge.

Towards the empirical analysis

Based on our review of the literature, we observe that available studies apply a variety of concepts, measures, predictors and objects in studying the fear of online crime. Building on these observations, the current study aims to provide further guidance to the study of (specific aspects of) fear of online crime in a more general sense. In so doing, we explicitly apply insights drawn from the fear of crime literature to the study of fear of online financial crime. A first step in our approach is to determine the degree to which – or, more specifically, the intensity with which – the Dutch general population reports fear of online financial crime. The current study also aims to assess the degree to which (the) victimization (thesis) as well as (the) vulnerability (thesis) explain fear of online financial crime, as reported by the general Dutch population. Whereas these surface as two important explanations in the literature, studies on fear of online financial crime report mixed results regarding the impact of these indicators. Extending the available literature in the cyber domain, the current study also considers the ways in which fear and behaviour are related. It is well recognized in the general fear of crime literature that fear may result in protective and avoidance behaviours (Liska et al., 1988). We also expect to find this mechanism in online contexts. More specifically, we will test this expectation by modelling fear of online crime as a possible determinant of the use of online services

(avoidance behaviour) and the application of online security measures (protective behaviour). In this line of reasoning, fear of crime is assumed to decrease regular online activities, for example purchasing and banking, and increase PC protection efforts. Below, then, we first address the methodological approach through which we seek to address our aims and test our expectations, followed by a description of our results.

Method

The data used in this study were collected in February 2016 and October 2016 by CentERdata, a Dutch research institute from Tilburg University specialized in data collection. The data are part of the fifth cycle of the LISS panel (see Van Wilsem, 2011, 2013, for publications on earlier waves). The LISS panel is an online panel in the Netherlands, consisting of 5000 households and comprising 8000 individuals. It is a representative sample of the Dutch household population (16 years and older), who were asked to complete a questionnaire on a variety of topics, such as offline and online victimization, PC protection efforts taken and fear of online crimes. In other months, they complete questionnaires on other topics, such as health, labour status and personality. In October 2016, the respondents participating in the LISS panel answered questions on Internet activities, such as online banking and Internet purchasing, and the devices used to go online. LISS panel respondents receive a small monetary compensation for their willingness to participate (€2.50 per 10 minutes, with monthly surveys usually taking no longer than 20 minutes). The surveys were distributed via an online questionnaire. For households that did not own a PC, temporary ownership of a PC was granted by CentERdata for the duration of cooperating with the LISS panel. The final response rate for the February 2016 questionnaire (on fear of online crime among other things) was 87.8 percent (which amounts to 6017 respondents from 4134 households). From this group, we excluded those who said they never went online (5.7 percent). This leaves us with a sample of 5673 respondents from the February 2016 sample. In addition, most analyses performed include data on devices and/or online activities from the October 2016 survey. This temporal order leads to some additional sample size loss ($N = 912$; 16 percent), which leaves us with 4761 respondents for the multivariate analyses.[4]

Dependent variables

Fear of online financial crime. The first part of the analysis of the data centres on fear of online financial crime, which is constructed as a scale variable consisting of the average value on four items (Cronbach's $\alpha = 0.79$). Participants were provided with the following propositions,[5] which they could score on a range from 1 (strongly disagree) to 5 (strongly agree):

– I am afraid that the things I buy over the Internet will not be delivered to me.
– I worry that my credit card number will become available to others via the Internet.
– I am afraid that someone will break into my computer.[6]
– I worry that through online banking my banking credentials will become available to others.

The wording on 'fear' and 'worry' in these questions flags the emotional dimension of the construct under study.[7] From the questions, it also follows that fear of online crime is studied as an 'intensity' measure, relating to particular types of cybercrime.

Online behaviours. The second part of the analysis focuses on determinants of online behaviour. The questionnaire asked if respondents could indicate whether they tend to spend time on the following online activities: 'online purchasing' and 'online banking'. Both questions could be answered with either 'yes' or 'no'; 89 percent confirmed they did for online banking, and 78 percent did for online purchasing. Furthermore, we also use information drawn from subsequent questions about how many hours in an average week the respondent devotes to these activities. Therefore, both online purchasing and online banking are operationalized in two ways: (a) whether or not they perform these activities, and (b) the amount of time they spend on them. Importantly then, whereas Hille et al. (2015) studied online purchase intention, here we study actual online behaviour, which Hille and colleagues also recommend as an avenue for further research.

Protective behaviours. The survey also presented six questions that considered the presence or absence of online security measures in terms of a firewall, virus scanner, anti-spyware, Trojan scanner or spam filter, as well as using a secured (coded) wireless network. We use these as dependent variables for protective behaviour, which distinguish respondents as users (1) and non-users (0).

Independent variables

Sociodemographic and personal characteristics. In line with studies discussed above, gender, age, education and income variables are also included in our analysis. The choice options for educational level were: 'elementary school' (1); VMBO – preparatory secondary vocational education (2); Havo/Vwo – general secondary education/preparatory scientific education (3); MBO – secondary vocational education (4); HBO – higher professional education (5); and 'university' (6). Age was measured by asking respondents to note their year of birth, which was recoded to age at the time of filling out the survey. For income, we asked for (self-reported) net household income. In order to reduce the skewness in the distribution of this variable, we performed a natural log transformation. A considerable proportion of the sample (9 percent) refused to give information on household income. We assigned them the average transformed value. Furthermore, we included a dummy variable on whether the respondent originally had a missing value. In this way, we keep this group in our analyses and are also able to examine whether or not the relationship of this group with the dependent variables is significantly different from that of those with a 'truly' average income.

Previous online victimization experience. Respondents were also asked about their own recent victimization experiences. They were asked if they had experienced during the past year (a) being hacked (1.5 percent), (b) being affected by a (digital) virus (3.5 percent), and (c) being defrauded online (3.0 percent).

**Table 1.** Descriptives of the dependent and independent variables.

Variable	Mean	SD	Min.	Max.	N
Dependent variables					
Fear of online financial crime	2.876	0.861	1	5	5404
Online purchasing (yes/no)	0.784		0	1	4761
Online banking (yes/no)	0.891		0	1	4761
No. of hours online purchasing per week	1.005	1.900	0	50	4753
No. of hours online banking per week	0.692	1.827	0	50	4752
Firewall	0.629		0	1	5673
Virus scanner	0.773		0	1	5673
Anti-spyware	0.431		0	1	5673
Trojan scanner	0.278		0	1	5673
Spam filter	0.576		0	1	5673
Security of wireless network at home	0.625		0	1	5673
Independent variables					
Female	0.533		0	1	5673
Age	50.35	17.898	16	98	5673
Educational level	3.690	1.503	1	6	5663
Net household income (LN)	7.775	0.968	0	12.12	5673
Missing value net household income (LN)	0.092	0.288	0	1	5673
No. of online computers in use in household	2.190	1.321	0	16	5673
Presence of computer or laptop	0.944		0	1	4967
Presence of tablet	0.579		0	1	4966
Presence of smartphone	0.666		0	1	4966
Victimization: Hacking last year	0.015		0	1	5390
Victimization: Virus on computer last year	0.035		0	1	5483
Victimization: Online fraud last year	0.030		0	1	5570

Online infrastructure. Apart from social vulnerability, respondents may fear online crime as a consequence of the potential exposure to online offenders. In order to take account of this possibility, we include the amount of hardware present in the household, because they are a proxy of the possibilities for going online. We therefore include in our analysis: (a) the number of PCs in the household, (b) the use of a PC or laptop, (c) the use of a tablet, and (d) the use of a smartphone.

Table 1 shows the descriptives of the dependent and independent variables used in this research.

Analysis strategy

We use several types of regression to assess the relationship between the dependent and independent variables. First, we report linear regression estimates for the model that treats fear of online financial crime as a function of background characteristics that indicate vulnerability, device possession and online victimization experiences. Results
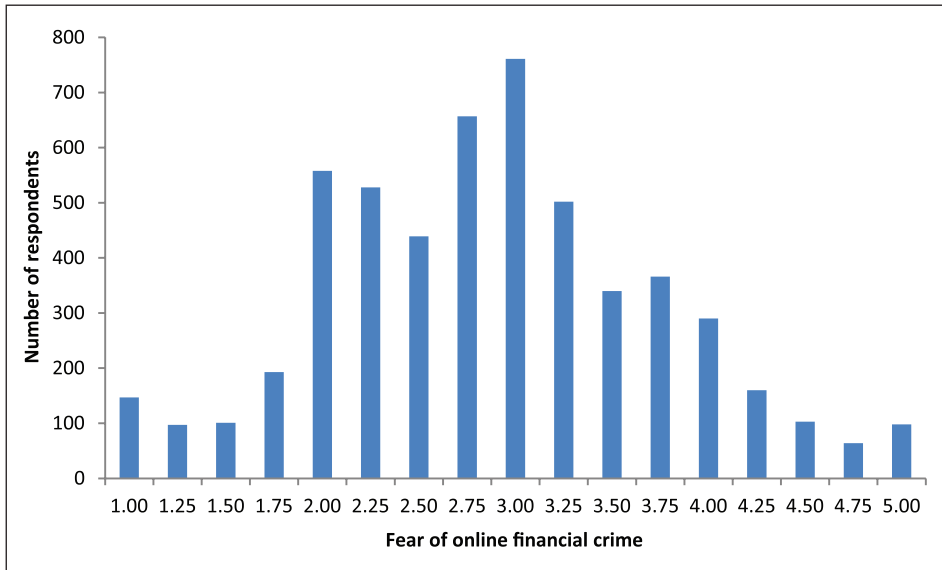
Figure 1. Histogram of the amount of fear of online financial crime (N = 5404).

were checked for normal distribution of residuals and homoscedasticity – two assumptions in linear regression modelling – and both were found to be in order. Secondly, the analyses that treat online activities (purchasing and banking) as dependent variables employ two types of regression modelling: logistic (on whether or not respondents perform this activity) and negative binomial (on how many hours per week, on average, respondents devote to it). Considering the highly skewed nature of the latter variables (counts, with many respondents reporting few or an intermediate amount of hours, and a small group devoting a considerable amount of time to it), negative binomial models are the most suitable option (Osgood, 2000). Finally, the last set of regression analyses treat (dichotomous) PC security measures taken as dependent variables; logistic regression is used here. All models were checked for multicollinearity, which was found to be not an issue considering that VIF values nowhere exceeded 1.5.

Results

To what extent do members of the Dutch general public express fear of online financial crime?

Figure 1 provides a histogram of the scores on our dependent variable: fear of online financial crime. On average, members of the Dutch general public report an intermediate level of fear of 2.88 on the scale, ranging from 1 to 5, used for the current study. Underlying this scale variable are different scores on the separate variables on fear. Approximately 21 percent of the respondents (strongly) agree with the item on being afraid that products purchased online will not be delivered; 25 percent of the respondents

Table 2. OLS regression of fear of online financial crime on sociodemographic characteristics, computer use and online victimization.

	Model 1		Model 2	
	B	SE	B	SE
Intercept	2.685***	0.117	2.752***	0.129
Female	0.098***	0.025	0.105***	0.025
Age	0.010***	0.001	0.009***	0.001
Educational level	−0.037***	0.008	−0.031***	0.008
Household income (LN)	−0.036**	0.014	−0.017	0.014
Missing value household income	0.063	0.044	0.064	0.044
No. of PCs in household			−0.029**	0.010
Ownership of PC or laptop			−0.031	0.057
Ownership of tablet			−0.031	0.027
Ownership of smartphone			−0.118***	0.030
Victim: Hacking			0.567***	0.105
Victim: Infection by virus			0.283***	0.071
Victim: Online fraud			0.193***	0.074
N	4508		4508	
R^2	.055		.075	
F(df)	52.54 (5)		30.504 (12)	

*$p < .05$, **$p < .01$, ***$p < .001$

(strongly) agree that they worry their credit card number can be traced via the Internet; in addition, 31 percent indicate they are afraid their PC will be hacked/accessed; finally, 28 percent (strongly) agree they worry their banking credentials will become available to others through online banking.

Regression analyses: Which people experience fear of online financial crime?

Table 2 provides an overview of the results derived from two consecutive OLS regression models on fear of online financial crime. Model 1 treats this fear as a function of sociodemographic characteristics. Model 2 adds device possession and online victimization experiences to the equation. From Model 1, several interesting findings can be derived. Higher levels of fear of online financial crime are found for females and elderly people. Also, lower levels of fear are found for the higher educated and for members of

high-income households. As we add the additional covariates in Model 2, the effects of these sociodemographic predictors are not affected substantially, with the exception of the income effect – which reaches non-significance. Furthermore, Model 2 shows that all victimization experiences included in the model – being hacked, being infected by a computer virus and being defrauded online – go together with higher levels of fear of online crime.

The indicators of device possession show either a small or no relationship with online fear. Levels of fear are somewhat lower with a higher number of PCs in the household and if one uses a smartphone. Possibly, rather than being an indicator of exposure to risk, device possession may indicate confidence in online skills and a low perceived risk of victimization.

Regression analyses: Is fear of online financial crime accompanied by lower levels of online banking and purchasing?

Our next step is to determine the way in which fear of online financial crime, along with other mechanisms, correlates with regular online behaviours. For this, we use the same covariates as in Model 2 of Table 2 and add fear of online financial crime. This model is used to explain which people engage in online purchasing and online banking (Table 3). For both behaviours, we consider whether or not people engage in that activity (logistic regression) and how many hours per week they devote to it (negative binomial model).
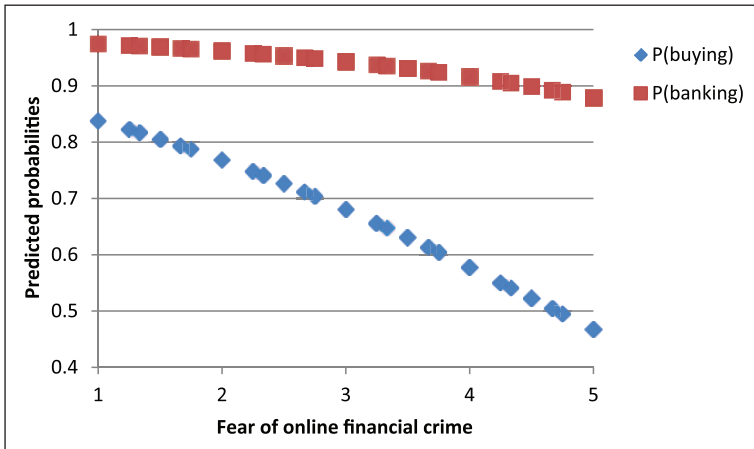
For purchasing, several patterns emerge. First of all, with respect to sociodemographic characteristics, online purchasing is done more often by young people and by the higher educated. Computer usage also appears to be important, as higher probabilities of Internet shopping is found for members of households with many PCs, PC/laptop owners, tablet owners, and smartphone owners. Purchasing *intensity* in terms of hours per week is lower among older people and is (positively) related to the number of PCs. Furthermore, with regard to victimization experiences, the single significant relationship was found for infection by a PC virus. Though the direction of the coefficient may suggest reversed causality, with victims showing higher purchasing intensity, it is relevant to point out the time order in which the information was collected, with victimization experiences (February 2016) asked at an earlier moment than online activities (October 2016). Certainly, for future research it would be relevant to examine whether the victimization experience was accompanied by a *change* in purchasing activity. Finally, in line with our expectations, fear of online financial crime goes together with smaller probabilities of engaging in online purchasing, as well as a smaller number of hours.

For online banking, the second part of Table 3, we find similarities as well as some differences compared with the purchasing models discussed above. Again, older people refrain more from banking online, but when they do use online banking they tend to put in more time. Furthermore, the possession of computer devices goes together with greater probabilities of doing online banking, but not with greater intensity of use. With respect to victimization experiences (again, measured prior to the online activity), we find some mixed results. Being hacked is slightly negatively related to the decision to bank or not (but not to intensity of use), whereas virus infection and online fraud victimization are

Table 3. Logistic regression and negative binomial models of online behaviour (purchasing and banking) on sociodemographic characteristics, computer use, online victimization and fear of online financial crime.

| | Online purchasing | | | | Online banking | | | |
| | Logistic regression (No/Yes 0/1) | | Negative binomial model (No. hrs/week) | | Logistic regression (No/Yes 0/1) | | Negative binomial model (No. hrs/week) | |
	B	SE	B	SE	B	SE	B	SE
Intercept	1.394**	0.515	−0.018	0.279	3.531	0.872	−0.193	0.257
Female	−0.046	0.088	0.002	0.049	−0.104	0.112	0.009	0.044
Age	−0.038***	0.003	−0.011***	0.002	−0.022***	0.004	0.004**	0.001
Educational level	0.328***	0.030	0.017	0.017	0.330***	0.039	−0.005	0.015
Household income (LN)	0.081	0.052	0.007	0.026	−0.211*	0.101	−0.011	0.025
Missing value household income	−0.574***	0.147	−0.124	0.088	−0.238	0.191	−0.073	0.079
No. of PCs in household	0.183***	0.043	0.049**	0.019	0.130*	0.056	0.012	0.018
Ownership of PC or laptop	0.656**	0.220	0.208	0.143	0.917***	0.246	0.204	0.128
Ownership of tablet	0.439***	0.091	0.035	0.053	0.350**	0.117	−0.004	0.047
Ownership of smartphone	0.775***	0.093	−0.048	0.060	0.754***	0.121	−0.077	0.052
Victim: Hacking	−0.619	0.327	0.190	0.195	−0.773*	0.385	0.181	0.178
Victim: Infection by virus	0.369	0.294	0.489***	0.124	0.307	0.393	0.406**	0.119
Victim: Online fraud	0.670	0.354	0.195	0.132	1.567*	0.725	0.077	0.128
Fear of online financial crime	−0.443***	0.052	−0.102**	0.030	−0.417***	0.065	−0.039	0.027
N	4351		4343		4351		4344	
Nagelkerke R^2	0.310		—		0.193		—	
Likelihood ratio X^2 (df = 13)	—		131.061***		—		34.613***	

$*p < .05, **p < .01, ***p < .001$

Figure 2. Visualization of the predicted probabilities (ceteris paribus) of online purchasing and banking.

positively related to banking (virus infection to intensity, fraud to the decision to do online banking or not). Finally, higher levels of fear of online financial crime go together with a lower probability of engaging in online banking, but not of intensity of use.[8]

One of the central findings mentioned above concerns the restricting force of fear of online financial crime on online purchasing and banking. In order to make clearer the magnitude of this relationship, we calculated the predicted probabilities of online purchasing and banking as a function of fear of online financial crime (as shown in the logistic regression analyses in Table 3), and visually plot them. These predicted probabilities are the outcome of the intercepts and the regression coefficients for online fear; we fix the values of the other independent variables at certain, predetermined levels.[9] Figure 2 shows how the predicted probabilities of both online purchasing and banking drop with increasing levels of fear, especially for those who are very fearful: whereas respondents with minimum levels of fear have predicted probabilities of banking of well over 90 percent and purchasing of over 80 percent, for those at the other end of the fear spectrum (4 to 5 on our scale), these probabilities drop approximately 10 percentage points for online banking and up to 35 percentage points for online purchasing.

Regression analyses: Are fear of online financial crime and PC protection behaviour connected?

To conclude our exploration of the potential consequences of fear of online financial crime, we examine the relationship with several protective behaviours aimed at enhancing PC security. For this, we relate background characteristics, possession of computer devices, victimization experiences and fear to respondents' accounts of whether they employed protective behaviours: a firewall, virus scanner, anti-spyware, Trojan scanner, spam filter and securing the wireless network at home (Table 4). For all protective

Table 4. Logistic regression of PC preventive measures on sociodemographic characteristics, computer use, online victimization and fear of online financial crime.

	Firewall		Virus scanner		Anti-spyware		Trojan scanner		Spam filter		Security wireless network	
	B	SE	B	SE	B	SE	B	SE	B	SE	B	SE
Intercept	-0.612	0.361	-0.693	0.390	-0.692*	0.347	-1.179**	0.372	-1.639***	0.344	0.494	0.370
Female	-0.832***	0.068	-0.463***	0.078	-0.868***	0.064	-0.842***	0.070	-0.395***	0.064	-0.577***	0.069
Age	-0.004	0.002	0.003	0.002	0.002	0.002	-0.004*	0.002	0.007**	0.002	-0.023***	0.002
Educational level	0.187***	0.023	0.156***	0.026	0.125***	0.022	0.158***	0.024	0.185***	0.022	0.154***	0.023
Household income (LN)	-0.004	0.037	0.047	0.040	-0.072*	0.036	-0.055	0.037	0.063	0.035	0.028	0.038
Missing value household income	-0.129	0.116	0.007	0.134	0.021	0.112	0.173	0.119	-0.073	0.111	-0.199	0.118
No. of PCs in household	0.219***	0.030	0.201***	0.036	0.177***	0.026	0.172***	0.027	0.155***	0.027	0.226***	0.031
Ownership of PC or laptop	0.433**	0.145	0.418**	0.152	0.142	0.149	0.035	0.168	0.468**	0.142	0.266	0.149
Ownership of tablet	0.290***	0.071	0.176*	0.081	0.167*	0.068	0.186*	0.075	0.174*	0.068	0.426***	0.071
Ownership of smartphone	0.383***	0.078	0.411***	0.089	0.287***	0.077	0.150	0.085	0.225***	0.076	0.341***	0.078
Victim: Hacking	-0.005	0.286	-0.079	0.331	-0.458	0.275	-0.280	0.305	-0.436	0.268	-0.377	0.275
Victim: Infection by virus	-0.052	0.191	0.439	0.253	0.368*	0.178	-0.090	0.195	0.155	0.183	-0.455*	0.188
Victim: Online fraud	0.043	0.205	-0.245	0.227	0.119	0.187	0.030	0.198	-0.108	0.188	-0.028	0.208
Fear of online financial crime	-0.021	0.040	0.011	0.046	0.024	0.038	0.026	0.042	-0.098*	0.038	-0.112*	0.041
N	4508		4508		4508		4508		4508		4508	
Nagelkerke R²	.137		.073		.102		.093		.079		.176	

*p < .05, **p < .01, ***p < .001

behaviours, adoption is higher among men, the higher educated, and people with many computers in their household. Furthermore, victimization experiences were not significantly related to protective measures, with the exception of virus infection, and slightly related to a lower probability of wireless network securing. Finally, fear of online financial crime showed little significant relationship to protective measures. Small but significant negative relationships (that is, not in the expected direction) were found between fear and adopting a spam filter and securing one's wireless network.

Conclusion and discussion

Against a background of public and academic interest in the ways Internet-related threats and dangers permeate people's everyday lives, and society more generally, the current study took particular interest in investigating fear of online crime among the general Dutch population and the ways this is related to online protective and avoidance behaviour. More specifically, the current study investigated fear of online financial crime, its correlates, and how it is related to online purchasing, online banking and the application of PC security measures. Although many before us have studied people's fear of crime, including the links between fear and protective and avoidance behaviours, this is not the case for fears of online crime. In fact, in the recent *Routledge International Handbook on Fear of Crime*, a case is made by Brunton-Smith (2018) for paying greater attention to the online dimensions of fear of crime in a more general sense (see also Henson and Reyns, 2015). It is important to study (online) fear of crime, because it is generally acknowledged that fear of crime affects people's well-being negatively (Doran and Burgess, 2012). At the same time, it is important to further investigate the links between fear and behaviour in online (consumer) contexts because, according to Roberts et al. (2013: 324, citing Lynch, 2005), fear of cybercrime might damage 'consumer trust and confidence in using the Internet', which is likely to have important implications for e-commerce and – maybe more important – people's capacity to use the Internet freely.

Our findings on a sample that was representative of Dutch households show an intermediate level of fear of online financial crime. This means that around 20–30 percent of our sample tend to (strongly) agree with the propositions, stating that they do fear or worry about particular forms of online financial crime. This figure aligns well with the results in the European Commission report on 'Europeans' attitudes towards cyber security', where 36 percent (EU average, 42 percent) of the Dutch participants are concerned about the security of online payments, and 30 percent (EU average, 23 percent) are afraid they will not receive the goods or services they buy online (European Commission, 2017).

Beyond providing a general measure of the intensity of fear about online financial crime, the current study also sought to explain variations in reported fear levels. Explanations centring on the vulnerabilities model – approached through proxies such as gender, educational level and age – and the victimization model perform quite well. In particular, those who have been the victim of hacking and/or have been infected by a computer virus report significantly higher fear of online financial crime. This is also the case for older Dutch people and for lower-educated inhabitants of the Netherlands.

Perhaps most interesting, however, are the clear and quite robust links outlined in our results between fear of online financial crime and online purchasing and online banking, even when accounting for a range of other variables (sociodemographic characteristics, device possession and victimization experiences). In fact, we find fear of online financial crime to have a clear and negative relationship to regular Internet behaviour in our models, with lower engagement in purchasing and banking for those who are more fearful. As such, the results are in line with the literature that associates fear of crime with avoidance behaviour (Liska et al., 1988; Rader, 2004; Rader et al., 2007). On a more general level, we take this finding to be in line with those presented by Hille et al. (2015). Yet, instead of focusing on online purchase *intention* (see Hille et al., 2015), we have estimated fear of online financial crime vis-à-vis actual Internet behaviour. Indications that fear is related to the application of protective behaviours on one's personal computer (installing a firewall, virus scanner, anti-spyware, Trojan scanner, spam filter and/or using a secured (coded) wireless network) were largely absent in our data, however.

Interpreting the above, it should nonetheless be taken into account that the variance explained by our models is modest at best. This is especially the case for the model explaining fear of online financial crime, meaning many other variables are in play explaining our respondents' fears of online crime not accounted for in the current study. This also flags up that studies – including this one – have started to get (further) at the complexity of explaining fear of online crime, but they might still learn valuable lessons by looking at (developments that are part of) their offline equivalents (see, especially, Farrall et al., 2012; Hale, 1996; Lee and Mythen, 2018; Spithoven, 2017) and further integrate, test and re-work perspectives and theories from that strand of literature. As mentioned earlier, the offline literature differentiates between risk perceptions of crime and crime fear/worry, mutually affecting one another. It is also well known in the literature that (popular) representations of crime (for instance in the media, but also in interpersonal communications) affect fear of crime (Farrall et al., 2012) and possibly also Internet behaviours such as purchasing and banking. More generally, the current study has not given much thought to the ways in which fear of (online) crime may also be socially constructed and related to broader socio-political contexts (Lee, 2001; Pain, 2000, 2009). Although we could not account for such aspects using our current dataset, it would be interesting to include them in future studies. In addition, it would be interesting to investigate not only the intensity of fear of online crime (studied here) but also the frequency with which people actually worry about cybercrime, and to consider whether or not such events (of worry) are linked to particular and concrete circumstances. Using such a framework, we might also and more clearly integrate the role of the (digital) 'environment', which in its own right is an important predictor of fear of crime in the sub-discipline of environmental criminology (see, for instance, Brunton-Smith et al., 2013). It would also be interesting for future studies to study the degree to which reported levels of fear of online crime (such as those above) may also and in fact be functional (Jackson and Gray, 2010; Warr, 2000), because it may keep potential victims from risky situations. This could especially be the case if people structurally underestimate the risks of falling victim to (cyber)crime (Melde et al., 2016; Warr, 2000). Finally, the literature also illustrates the importance of crime-specific studies into fear of crime. As mentioned, we focused only on fears of online financial crimes. Examining other crime types, and

drawing comparisons between them, would be interesting and necessary to understand fear of online crime in a more comprehensive manner.

It can also be noted that longitudinal research in the fear of online crime literature is in short supply, but would clearly help in terms of how variables are interrelated and causally aligned, thereby providing a clear temporal order. Here, we were able to tease out the temporal order between fear/victimization and Internet activity, because the former was asked six months earlier. Nevertheless, in testing hypotheses on the impact of victimization on fear, and of fear on Internet activities, future work should be done on *changes* in dependent and independent variables. Does a victimization experience lead to an increase in fear? And do increases in fear go together with declining Internet activity? Better understanding the causality of the relationships outlined in this study would help us to better understand the ways in which emotion and behaviour are linked. Specifically, it would increase our understanding of the escalating feedback loop that Liska et al. (1988) proposed – here, specifically for the online context – and the ways in which behaviour (may) in turn also affect(s) fear of crime (Rader, 2004; Rader et al., 2007).

Whereas other studies, then, have referred to aversive behavioural aspects of negative emotional experiences with online crime, the current study has empirically studied and investigated these links. Even though the Internet augments the agency of individuals in many different ways, we take it that the current study also and more generally substantiates claims made in the literature that fear of (online) crime can and does quite literally negatively impact on the daily lives of individuals. In so doing, this study contributes to a developing field of studies into the subjective dimensions of Internet-related crime and suggests that negative experiences with the Internet, including fear of online crimes, may obstruct individuals' perceived online freedom, opportunities and liberties.

Acknowledgements

Funding

Notes

1. Importantly, however, Yar (2009: 108) rightly argues that this is a question of balance, where (reactions to) fear and worry about online crimes should be not prioritized over, but carefully balanced against, 'the potentially positive, enabling, empowering and otherwise life-enhancing opportunities that the Internet may present for many users'.
2. But see Henson and Reyns (2015) and Jackson and Gray (2010), who argue that some degree of fear may also be functional, because it may keep potential victims from risky situations.
3. See Farrall et al.'s (2012) book *Social Order and the Fear of Crime in Contemporary Times*, as well as the recent *Routledge International Handbook on Fear of Crime* (Lee and Mythen, 2018) and Hale's (1996) review of the fear of crime literature for a more extensive discussion.
4. The group for which February and October 2016 data are combined differs slightly yet significantly from the group that participated only in February 2016. October 2016 data on online

activities were somewhat more frequently missing among men, younger people, the lower educated and those with higher incomes.

5. Whereas studies more often directly ask the degree to which respondents worry about or fear a particular type of online crime, proposition formulations are a generally accepted (if other) means of questioning in the social sciences, including studies on fear of (online) crime (see, for instance, Hille et al., 2015; Rader et al., 2007).

6. Although this item does not directly refer to financial crimes, the modus operandi of several online financial crimes starts with a cyber-offender hacking the target's computer, for example to steal personally identifying information. Furthermore, the scale variable lost reliability if this item was omitted, dropping to $\alpha = 0.72$. Therefore, for substantive and empirical reasons, we chose to include this item in our scale variable on online fear. Nevertheless, all analyses were also run with this item omitted in order to explore whether this yielded substantially different results, which turned out not to be the case. At one point, the alternative analyses showed a significant effect for fear, whereas the currently reported result does not. Our results section will make mention of this difference.

7. Although the terms 'fear' and 'worry' are frequently used to measure the fear of crime, it should be noted that the terms should not be considered entirely exchangeable (see Jackson and Gouseti, 2013), which amounts to a flaw in our research design.

8. Here, we find a different result if we use a three-item dependent scale variable (with the item on hacking omitted) instead of the current four-item scale (see note 6). This alternative scale variable yields a significant negative relationship (that is, in the expected direction), with fear going together with lower banking intensity.

9. Here, we calculate the predicted probabilities for someone who is male, is aged 50, has an intermediate level of education (3 on our scale), has average (LN) income, has two computers, possesses a laptop, tablet and smartphone, and has no victimization experiences.

References

Böhme R and Moore T (2012) How do consumers react to cybercrime? In: *2012 eCrime Researchers Summit*, Las Croabas, USA, 23–24 October 2012, 1–12. DOI: 10.1109/eCrime.2012.6489519.

Brenner SW (2014) *Cyberthreats and the Decline of the Nation-state*. Abingdon: Routledge.

Brunton-Smith I (2018) Fear 2.0: Worry about cybercrime in England and Wales. In: Lee M and Mythen G (eds) *The Routledge International Handbook on Fear of Crime*. Abingdon: Routledge.

Brunton-Smith I, Sutherland A and Jackson J (2013) The role of neighbourhoods in shaping crime and perceptions of crime. In: Manley D, Van Ham M, Bailey N, et al. (eds) *Neighbourhood Effects or Neighbourhood Based Problems? A Policy Context*. Dordrecht: Springer, 67–87.

Doran BJ and Burgess MB (2012) Why is fear of crime a serious social problem? In: Doran BJ and Burgess MB (eds) *Putting Fear of Crime on the Map*. New York: Springer, 9–23.

European Commission (2015) *Special Eurobarometer 431: Data Protection*. Report, European Commission, June.

European Commission (2017) *Special Eurobarometer 464a: Europeans' Attitudes towards Cyber Security*. Report, European Commission, September.

Eurostat (2018) Households – level of Internet access. URL (accessed 7 March 2019): https://ec.europa.eu/eurostat/web/products-datasets/product?code=ISOC_CI_IN_H.

Farrall S and Gadd D (2004) Evaluating crime fears: A research note on a pilot study to improve the measurement of the 'fear of crime' as a performance indicator. *Evaluation* 10(4): 493–502.

Farrall SD, Jackson J and Gray E (2012) *Social Order and the Fear of Crime in Contemporary Times*. Oxford: Oxford University Press.

Fattah EA (1993) Research on fear of crime: Some common conceptual and measurement problems. In: Bilsky W, Pfeiffer C and Wetzels P (eds) *Fear of Crime and Criminal Victimization*. Stuttgart: Ferdinand Enke Verlag, 45–70.

Ferraro KF and LaGrange RL (1987) The measurement of fear of crime. *Sociological Inquiry* 57(1): 70–97.

Forsythe SM and Shi B (2003) Consumer patronage and risk perceptions in Internet shopping. *Journal of Business Research* 56(11): 867–875.

Gray E, Jackson J and Farrall S (2012) In search of the fear of crime: Using interdisciplinary insights to improve the conceptualization and measurement of everyday insecurities. In: Gadd D, Karstedt S and Messner S (eds) *Sage Handbook of Criminological Research Methods*. London: Sage, 266–281.

Hale C (1996) Fear of crime: A review of the literature. *International Review of Victimology* 4(2): 79–150.

Henson B and Reyns BW (2015) The only thing we have to fear is fear itself … and crime: The current state of the fear of crime literature and where it should go next. *Sociology Compass* 9(2): 91–103.

Hille P, Walsh G and Cleveland M (2015) Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing* 30(May): 1–19.

Hinkle JC (2015) Emotional fear of crime vs. perceived safety and risk: Implications for measuring 'fear' and testing the broken windows thesis. *American Journal of Criminal Justice* 40(1): 147–168.

Holt TJ and Bossler AM (2008) Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behaviour* 30(1): 1–25.

Holt TJ and Bossler AM (2014) An assessment of the current state of cybercrime scholarship. *Deviant Behaviour* 35(1): 20–40.

Jackson J (2005) Validating new measures of the fear of crime. *International Journal of Social Research Methodology* 8(4): 297–315.

Jackson J (2009) A psychological perspective on vulnerability in the fear of crime. *Psychology, Crime & Law* 15(4): 365–390.

Jackson J and Gouseti I (2013) Fear of crime: An entry to the Encyclopedia of theoretical criminology. In: Mitchell Miller J (ed.) *Encyclopedia of Theoretical Criminology*. Oxford: Wiley-Blackwell, forthcoming. URL (accessed 7 March 2019): SSRN: https://ssrn.com/abstract=2118663.

Jackson J and Gray E (2010) Functional fear and public insecurities about crime. *British Journal of Criminology* 50(1): 1–22.

Jansen J, Kop N and Stol W (2017) Internetbankieren: Veiligheidspercepties van gebruikers. *Tijdschrift voor Veiligheid* 16(1): 36–51.

Lee M (2001) The genesis of 'fear of crime'. *Theoretical Criminology* 5(4): 467–485.

Lee M and Mythen G (2018) *The Routledge International Handbook on Fear of Crime*. Abingdon: Routledge.

Leukfeldt ER (2015) Comparing victims of phishing and malware attacks. Unraveling risk factors and possibilities for situational crime prevention. *International Journal of Advanced Studies in Computer Science and Engineering* 4(5): 26–32.

Liska AE, Sanchirico A and Reed MD (1988) Fear of crime and constrained behaviour: Specifying and estimating a reciprocal effects model. *Social Forces* 66(3): 827–837.

Lorenc T, Clayton S, Neary D, et al. (2012) Crime, fear of crime, environment, and mental health and wellbeing: Mapping review of theories and causal pathways. *Health & Place* 18(4): 757–765.

Lynch J (2005) Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks. *Berkeley Technology Law Journal* 20(259): 259–300.

Melde C, Berg MT and Esbensen FA (2016) Fear, social interactions, and violence mitigation. *Justice Quarterly* 33(3): 481–509.

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

Osgood DW (2000) Poisson-based regression analysis of aggregate crime rates. *Journal of Quantitative Criminology* 16(1): 21–43.

Pain R (2000) Place, social relations and the fear of crime: A review. *Progress in Human Geography* 24(3): 365–387.

Pain R (2009) Globalized fear? Towards an emotional geopolitics. *Progress in Human Geography* 33(4): 466–486.

Powell AL (2013) Computer anxiety: Comparison of research from the 1990s and 2000s. *Computers in Human Behaviour* 29(6): 2337–2381.

Rader NE (2004) The threat of victimization: A theoretical reconceptualization of fear of crime. *Sociological Spectrum* 24(6): 689–704.

Rader NE, May DC and Goodrum S (2007) An empirical assessment of the 'threat of victimization': Considering fear of crime, perceived risk, avoidance, and defensive behaviours. *Sociological Spectrum* 27(5): 475–505.

Reid LW, Robert JT and Hilliard HM (1998) Fear of crime and collective action: An analysis of coping strategies. *Sociological Inquiry* 68(3): 312–328.

Reisig MD, Pratt TC and Holtfreter K (2009) Perceived risk of Internet theft victimization. *Criminal Justice and Behaviour* 36(4): 369–384.

Reyns BW (2015) A routine activity perspective on online victimization. *Journal of Financial Crime* 22(4): 396–411.

Riek M, Böhme R and Moore T (2016) Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing* 13(2): 261–273.

Roberts LD, Indermaur D and Spiranovic C (2013) Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law* 20(3): 315–328.

Spithoven R (2017) *Keeping Trouble at a Safe Distance: Unravelling the Significance of 'the Fear of Crime'*. The Hague: Eleven Publishing.

Starkweather S (2007) Gender, perceptions of safety and strategic responses among Ohio University students. *Gender, Place and Culture* 14(3): 355–370.

Van Wegberg RS, Klievink AJ and Van Eeten MJG (2017) Discerning novel value chains in financial malware. *European Journal on Criminal Policy and Research* 23(4): 575–594.

Van Wilsem J (2011) Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology* 8(2): 115–127.

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

Virtanen SM (2017) Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law* 24(3): 323–338.

Warr M (2000) Fear of crime in the United States: Avenues for research and policy. *Criminal Justice* 4(4): 451–489.

Yar M (2009) Public perceptions and public opinion about Internet crime. In: Jewkes Y and Yar M (eds) *Handbook of Internet Crime*. London: Willan, 104–119.

Yar M (2013) *Cybercrime and Society*. London: SAGE.

Yu S (2014) Fear of cyber crime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology* 8(1): 36–46.