Reporting cybercrime victimization: determinants, motives, and previous experiences

Published in:
Policing

Publication status and date:
Published: 02/03/2020

DOI (link to publisher):
10.1108/PIJPSM-07-2019-0122

Document Version
Publisher's PDF, also known as Version of record

Document License/Available under:
Article 25fa Dutch Copyright Act

Citation for the published version (APA):
van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing*, *43*(1), 17-34. https://doi.org/10.1108/PIJPSM-07-2019-0122

Reporting cybercrime victimization: determinants, motives, and previous experiences

Steve van de Weijer
Netherlands Institute for the Study of Crime and Law Enforcement, Amsterdam, Netherlands
Rutger Leukfeldt
Netherlands Institute for the Study of Crime and Law Enforcement, Amsterdam, Netherlands and The Hague University of Applied Sciences, Den Haag, Netherlands, and
Sophie Van der Zee
Erasmus University Rotterdam, Rotterdam, Netherlands

Received 30 July 2019
Revised 25 October 2019
12 December 2019
Accepted 13 December 2019

Abstract

Purpose – Cybercrime rates have increased rapidly during the last couple of decades, resulting in cybercrimes becoming common crimes. However, most victims do not report cybercrimes to the police. Therefore, this study examines reporting cybercrime victimization and provides insights into the role of the police in this process.
Design/methodology/approach – A sample of 595 individuals was used. All respondents were shown three vignettes about hypothetical cybercrime victimization and were asked to imagine that this situation happened to them. Four crime and reporting characteristics were manipulated across vignettes. Respondents' intentions to report to the police and to other organizations were used as the dependent variables in regression analyses. Four random factors in the vignettes (i.e. type of crime, seriousness of crime, victim–perpetrator relationship, and reporting modality), as well as several characteristics of the respondents were included in the regression models as independent variables.
Findings – The type of cybercrime is the most important predictor for reporting behaviors. Other determinants are: more serious offenses were more often reported and offenses are less often reported in situations where the victim personally knows the perpetrator. Furthermore, there is large discrepancy between intended and actual cybercrime reporting. These findings provide valuable insights into the factors that influence reporting behavior in the real world. Only a fifth of respondents indicated that they would not report cybercrime victimization to the police. This implies that attempts at improving reporting rates should not solely be focused on improving people's attitudes, but also on removing obstacles to turn these attitudes into actions.
Originality/value – In the current study, the authors contribute to the existing literature by asking a large sample from the general population in the Netherlands about both their intended reporting behavior (i.e. a vignette study) and their actual reporting behavior (i.e. self-reports) of victimization of a wide variety of different types of cybercrime. Determinants of both reporting to the police as well as to other organizations are examined. Moreover, respondents are asked about motivations behind their decision to (not) report a cybercrime to the police. Last, people were asked about their past experiences with reporting cybercrime victimization to the police.

Keywords Cybercrime, Victimization, Reporting, Policing
Paper type Research paper

Introduction

Cybercrime rates have increased rapidly during the last couple of decades, resulting in cybercrimes becoming common crimes (CBS, 2018a). Self-report studies show that, in 2017, 11 percent of the Dutch population became a victim of a cybercrime, such as online consumer fraud (3.9 percent), online stalking (0.8 percent), and identity fraud (0.4 percent). Hacking is

This study was funded by Dutch research fund 'Politie en Wetenschap' [Police and Science].

1363-951X
DOI 10.1108/PIJPSM-07-2019-0122

now even the most common crime in the Netherlands, the country on which the current study focuses, with 5–6 percent of the citizens becoming a victim of hacking each year (CBS, 2018a). Figures from self-report data from other European countries show similar patterns (see, e.g. ONS (2016) for UK numbers on online fraud, malware, and hacking).

Although cybercrimes are becoming more common, the police experience difficulties in handling cybercrime. Previous studies show that law enforcement agencies in countries such as the Netherlands, England, Wales, and Australia are actually not handling cybercrimes very well (e.g. Bossler *et al.*, 2019; Leukfeldt *et al.*, 2018, 2019; Cross *et al.*, 2016). According to these studies, the police have a lack of knowledge when it comes to the fight against cybercrime. There is, however, another problem: most victims do not even report cybercrimes to the police. In the Netherlands, only 13 percent of the cybercrime victims reported their victimization to the police in 2017 and of those cases, only 8 percent resulted in a criminal complaint (CBS, 2018a). Of the different types of cybercrime, hacking was reported the least often to the police (5 percent), but also online consumer fraud (19 percent) and identity fraud (16 percent) are usually not reported to the police. Qualitative studies on this topic show a similar picture: cybercrime victims often do not report their victimization and even when they are inclined to do so, they often do not know where to report (Burgard and Schlembach, 2013; Bidgoli, 2015).

Given these low reporting rates, it is remarkable that only a couple of studies have specifically examined which cybercrime victims report to the police and which motives influence whether a victim will or will not report their cybercrime victimization (van der Weijer *et al.*, 2018; Jong *et al.*, 2018). Gaining knowledge about determinants and motives for cybercrime reporting behaviors is important in order to take actions to increase these reporting rates. Informed crime statistics can help identify key problems, allocate resources, form policy, and ultimately, catch perpetrators. Therefore, the current study examines reporting cybercrime victimization and provides insights into the role of the police in this process. This study is based on the Dutch report about willingness to report cybercrime (Van de Weijer, Leukfeldt and Van der Zee, 2020).

Literature review

Although only few studies have examined the determinants of reporting cybercrime to the police, numerous articles were published on reporting victimization of traditional crimes to the police. A theoretical perspective that is often used in these studies is the rational economic perspective, in which it is assumed that a victim reports a crime to the police if the expected benefits of reporting exceed the expected costs (Goudriaan *et al.*, 2006). Possible benefits of reporting crime to the police can be financial (e.g. retrieve stolen goods, financial compensation by the perpetrator, compensation of the damage by the insurance company), but can also be a decreased probability of revictimization if the perpetrator gets prosecuted. On the other hand, the time and effort to report a crime to the police can be considered as potential costs, as well as fear of retaliation by the perpetrator (Goudriaan *et al.*, 2005). In line with this rational cost–benefit perspective, previous studies have shown that higher benefits tend to result in higher reporting rates. Specifically, serious offenses (e.g. with more financial damage) are more often reported to the police than less serious offenses (e.g. Baumer and Lauritsen, 2010; Goudriaan *et al.*, 2005; Kääriäinen and Sirén, 2011), and victims who have insurance against the damage are more likely to report their victimization (e.g. Goudriaan, *et al.*, 2005; Tarling and Morris, 2010). Reducing the costs of reporting can also increase reporting rates. A vignette study by Tolsma *et al.* (2012) showed that people are more willing to report a crime when this is possible over the phone or the Internet, reducing the time it costs to report a crime.

In addition to a cost–benefit calculation, also psychological factors could play a role in making the decision whether or not to report a crime to the police (Goudriaan *et al.*, 2006). For example, people who feel ashamed for their victimization may not report the crime, while victims who want retribution may be more likely to report to the police in order to get the perpetrator convicted. The relationship between the victim and offender may further influence reporting behavior. If the offender is someone that the victim personally knows, the victim might feel empathy for the offender and not report the crime to the police to avoid negative consequences for the offender. Alternatively, the victim may be afraid of retaliation by the perpetrator when reporting the crime to the police (Goudriaan *et al.*, 2005). Previous studies on crime reporting behavior show mixed results with respect to the relationship between victim and offender (e.g. Baumer and Lauritsen, 2010; Goudriaan *et al.*, 2004; Schnebly, 2008). Another factor that can influence reporting behaviors is the victims' trust in, and more positive attitudes toward, the police. Previous studies showed that victims with more trust and positive attitudes are more likely to report their victimization to the police (e.g. Goudriaan *et al.*, 2005; Guzy and Hirtenlehner, 2015; Slocum *et al.*, 2010).

Previous studies have also found several demographic factors to be related to crime reporting behavior. Generally, older victims more often report crime to the police than younger victims (e.g. Baumer and Lauritsen, 2010; Goudriaan *et al.*, 2004; Guzy and Hirtenlehner, 2015) and women are more likely to report their victimization than men (e.g. Baumer and Lauritsen, 2010; Schnebly, 2008), although a couple of studies found the contrary (e.g. Goudriaan *et al.*, 2004). Moreover, victims with a (marital) partner are more likely to report their victimization to the police than those without a partner (e.g. Baumer and Lauritsen, 2010; Goudriaan *et al.*, 2004; Schnebly, 2008). Finally, mixed results have been found in previous studies with respect to the associations of educational level and income with crime reporting behavior (e.g. Goudriaan *et al.*, 2006; Gutierrez and Kirk, 2017; Guzy and Hirtenlehner, 2015; Schnebly, 2008).

The aforementioned crime reporting studies, however, focus solely on *traditional* types of crime and do not examine crime reporting behaviors of victims of cybercrime. There is very limited research examining victim reports of cybercrime. Some only compared the reporting rates of different types of cybercrime (Domenie *et al.*, 2013; Veenstra *et al.*, 2015), while others focused on the needs of victims after victimization (Cross *et al.*, 2016; Jansen and Leukfeldt, 2018; Leukfeldt *et al.*, 2019). To date, little is known about the factors that are associated with reporting cybercrime to the police and about the motivations behind these reports. van der Weijer *et al.*, 2018 were the first to study the determinants of reporting cybercrime victimization to the police, using data on more than 97,000 Dutch individuals who became the victim of an offense between 2012 and 2015. They found some remarkable differences between the demographic and contextual factors related to reporting traditional crimes and reporting cybercrimes to the police. While female victims were more likely to report traditional crimes to the police, male victims more often reported cybercrime. In addition, while a higher income was positively related to reporting traditional crime victimization to the police, a negative association was found between income and reporting cybercrime victimization. Moreover, several neighborhood characteristics that were related to the reporting of traditional crimes were not associated with reporting cybercrime to the police. Importantly, the results of van der Weijer *et al.*, 2018 showed that cybercrimes are more often reported to other organizations than the police, underlining the importance of taking into account reporting behavior to other organizations as well. Although the study by van der Weijer *et al.*, 2018 provided valuable first insights into the determinants of reporting cybercrime victimization, it did not provide a complete overview since they only examined the victims of three types of cybercrime (i.e. hacking, consumer fraud, identity theft) and did not investigate the motivations for (not) reporting a crime.

Jong *et al.* (2018) did examine the motivations to report cybercrime to the police in a vignette study among 175 university students. A vignette study provides the opportunity to test the intention to report across multiple crimes and scenarios. Their results showed that the motivations to (not) report cybercrime victimization to the police were very similar to known motivations to report traditional crime victimization (Goudriaan and Nieuwbeerta, 2007). People were found to be more likely to intent to report a cybercrime to the police when it concerns a more serious offense and when the perpetrator is someone they know personally. No significant associations were found with reporting possibilities (e.g. at the police station, over telephone, or on the Internet), gender, age, and attitudes toward the police (Jong *et al.*, 2018). In this study also a limited number of different types of cybercrimes were studied (i.e. hacking, consumer fraud, malware), and the results based on a student sample might not be generalizable to the general population.

Current study

In the current study, we contribute to the existing literature by asking a large sample from the general population in the Netherlands about both their intended reporting behavior (i.e. a vignette study) and their actual reporting behavior (i.e. self-reports) after victimization of a wide variety of different types of cybercrime. The research questions are: Which offense and victim characteristics predict intended and actual reporting to the police and other organizations? What are the most important motivations to report a cybercrime to the police or not? What are victims' experiences with reporting cybercrime to the police?

Methods

Sample

In order to examine the factors that play a role in reporting cybercrime victimization, we designed a questionnaire, which was distributed among a sample from an existing online research panel, including Dutch-speaking citizens aged 18 years and older. Respondents answered the questionnaire online, in return for a gift voucher. The analytic sample included 595 individuals who answered the complete questionnaire[1]. Although the sample was drawn from the general population in the Netherlands, it was not completely representative for the Dutch population. First, older persons were overrepresented in the sample: 35 percent of the sample was 65 years or older, while this is only 19.2 percent in the Dutch population (CBS, 2019). The average age of the sample members was 57.20 years (std. dev.: 15.08; ranging from 18 to 88 years). Second, men were overrepresented as 338 sample members are men (56.8 percent) compared to 49.7 percent in the general population. Third, our sample members more often had a high educational level (44.5 percent) than the general population (30 percent) in the Netherlands (CBS, 2018b).

Vignettes

In the first part of the questionnaire, all respondents were shown three vignettes about hypothetical cybercrime victimization and were asked to imagine that this situation happened to them. Figure 1 shows an example of such a vignette. Four crime and reporting characteristics were manipulated across vignettes. First, the type of cybercrime was manipulated between vignettes, covering credit card fraud, online consumer fraud, malware, hacking, and online threats. The second manipulation concerned the seriousness

Someone has retrieved the details of your personal credit card via the internet and has charged 1000 euros.
You do not know the perpetrator personally.
If you want to report the crime to the police, this is possible over the phone or on the police station.

Figure 1.
Example of a vignette

of the offense: more versus less serious offenses. For example, 100 euro or 1,000 euro damage after credit card fraud. The third manipulation concerned the relationship between victim and offender: "you do not know who the perpetrator is," "you know the perpetrator personally," and "you do not know the perpetrator personally." The fourth and final manipulation concerned the modality of reporting cybercrime to the police: "on the police station," "over the phone or on the police station," and "on the Internet, over the phone or on the police station."

After reading each vignette, respondents were asked whether or not they would report this cybercrime to the police. They could answer on a five-point scale ranging from 1 "Certainly not" to 5 "Certainly." Respondents who scored 4 or 5 on this scale were asked for the most important motive to report the crime to the police, while respondents who scored 1 or 2 were asked for the most important motive to not report the crime. Tables II and III show the list of motives respondents could choose from. Next, respondents were also asked on a five-point scale whether they would report this crime to another organization than the police.

The respondents' intentions to report the cybercrime to the police and to other organizations were used as the dependent variables in ordinal logistic regression analyses, since these variables had an ordinal scale. The four random factors in the vignettes (i.e. type of crime, seriousness of crime, victim–perpetrator relationship, and reporting modality), as well as several characteristics of the respondents were included in the regression models as independent variables. Since each respondent answered questions on three different vignettes, observations were clustered within respondents. Robust standard errors that take into account this clustering were therefore calculated in order to control for this violation of the assumption of independent observations[2].

The independent variables include, first of all, the *age* and *gender* of the respondents. Next, *marital status* was included with four different answer categories: single (19.8 percent), living together with a (marital) partner (62.5 percent), not living together with a (marital) partner (11.8 percent), and widowed (5.9 percent). The independent variable *parenthood* was measured using three categories: no children (33.3 percent), children not living at home (48.1 percent), and children living at home (18.7 percent). *Educational level* was measured on an ordinal scale from 1 "primary school" to 7 "Master's degree," with an average of 4.95 (std. dev.: 1.52). Next, the respondents' *employment status* was divided in three categories: employed (45.5 percent), unemployed/studying (18.5 percent), and pensioned (36.0 percent). The independent variable *income* was measured as the personal monthly income before taxes, divided in 12 categories ranging from 1 "no income" to 12 "More than 10.000 euro." Multiple imputation was used to substitute 61 missing values (10.3 percent) on the income variable. Moreover, respondents were also asked about *previous cybercrime victimization* (see also section 3.3). Based on the information from these questions, a variable was computed with three categories: never a victim of cybercrime (49.1 percent), a victim of cybercrime but never reported it to the police (41.8 percent), and a victim of cybercrime and reported it to the police at least once (9.1 percent). *Attitudes toward the police* was measured using the mean score of nine different items on police functioning (CBS, 2018a). Respondents could answer on a five-point scale ranging from 1 "very unsatisfied" to 5 "very satisfied." These items had an excellent internal consistency as shown by the Cronbach's alpha of 0.92. An independent variable indicating *fear for cybercrime victimization* was measured using eight items on which the respondents could answer with a five-point scale ranging from 1 "Totally disagree" to 5 "Totally agree" (van 't Hoff-de Goede *et al.*, 2019). The internal consistency of these items was good, as indicated by the Cronbach's alpha of 0.88. For both the variables, attitudes toward the police and fear for cybercrime victimization, factor analyses were used to create factor scores for each respondent. The factor loadings and exact items can be found in the

	Model 1: Reporting to the police			Model 2: Reporting to other organizations		
	B	Robust S.E.	OR	*B*	Robust S.E.	OR
Type of crime:						
Credit card fraud	(ref.)			(ref.)		
Online consumer fraud	−1.29***	0.16	0.28	−0.14	0.13	0.87
Malware	−1.57***	0.16	0.21	−0.85***	0.13	0.43
Hacking	−0.99***	0.15	0.37	−0.79***	0.13	0.45
Online threat	−0.66***	0.16	0.52	−0.81***	0.14	0.44
Seriousness	1.05**	0.09	2.86	0.31***	0.09	1.36
Relation with offender:						
Identity of offender is unknown	(ref.)			(ref.)		
Offender is an acquaintance	−0.30**	0.12	0.74	−0.56***	0.11	0.57
Offender is a stranger	−0.02	0.11	0.98	−0.08	0.11	0.92
Reporting possibilities:						
Police office	(ref.)			(ref.)		
Police office and telephone	0.04	0.12	1.04	−0.01	0.11	0.99
Police office, telephone, and online	0.14	0.12	1.15	−0.06	0.11	0.94
Gender (male = ref.)	0.17	0.14	1.19	0.42**	0.14	1.52
Age	0.02***	0.01	1.02	0.02***	0.01	1.02
Marital status:						
Single	(ref.)			(ref.)		
Relationship, living together	−0.08	0.18	0.92	0.12	0.17	1.13
Relationship, not living together	−0.07	0.22	0.93	−0.43	0.23	0.65
Widow	−0.22	0.34	0.80	0.16	0.33	1.17
Children:						
No	(ref.)			(ref.)		
Yes, not living at home	0.11	0.17	1.12	−0.06	0.18	0.94
Yes, living at home	0.17	0.19	1.19	0.15	0.17	1.16
Education	0.08	0.05	1.08	0.05	0.05	1.05
Employment status:						
Employed	(ref.)			(ref.)		
Unemployed/studying	0.11	0.22	1.12	0.31	0.18	1.36
Pensioned	0.14	0.19	1.15	0.02	0.20	1.02
Income	−0.05	0.04	0.95	0.01	0.04	1.01
Previous cybercrime victimization:						
No	(ref.)			(ref.)		
Yes, never reported to police	−0.32*	0.13	0.73	0.32*	0.13	1.38
Yes, ever reported to police	0.50**	0.23	1.65	0.59*	0.24	1.80
Attitudes toward the police	0.16**	0.07	1.17	0.04	0.07	1.04
Fear for cybercrime victimization	0.17*	0.07	1.19	0.11	0.07	1.12
IT skill level	−0.09	0.11	0.91	0.22*	0.10	1.25
N vignettes	1.785			1.785		
N respondents	595			595		
Pseudo R^2			0.078			0.0421

Table I.
Ordinal logistic regression analyses on intentions to report cybercrime victimization

Appendix. Finally, respondents' *IT skill level* was measured by asking respondents which of the following statements applied most to them (Holt and Bossler, 2008): (1) "I can use the internet and commonly used software like Word and Excel, but I cannot solve computer problems myself" (44.4 percent), (2) "I can use several software programs and solve some

Table II. Motives to report to the police

	Total	Credit card fraud	Online consumer fraud	Malware	Hacking	Online threat
To prevent this from happening to me again	137 (11.8%)	25 (9.0%)	5 (2.6%)	20 (11.0%)	31 (12.7%)	56 (20.8%)
To prevent the perpetrator from doing this again to someone else	322 (27.6%)	71 (25.5%)	80 (41.6%)	65 (35.7%)	78 (31.8%)	28 (10.4%)
I want the perpetrator to be caught	437 (37.5%)	98 (35.3%)	61 (31.8%)	59 (32.4%)	83 (33.9%)	136 (50.6%)
To create a safer online environment	119 (10.2%)	16 (5.8%)	12 (6.3%)	27 (14.8%)	32 (13.1%)	32 (11.9%)
It is my duty to report crime	57 (4.9%)	19 (6.8%)	11 (5.7%)	5 (2.8%)	10 (4.1%)	12 (4.5%)
To get the damage compensated	78 (6.7%)	44 (15.8%)	22 (11.5%)	4 (2.2%)	8 (3.3%)	0 (0.0%)
Other	16 (1.4%)	5 (1.8%)	1 (0.5%)	2 (1.1%)	2 (1.2%)	5 (19%)
Total	1.166 (100%)	278 (100%)	192 (100%)	182 (100%)	245 (100%)	269 (100%)

Table III. Motives to not report to the police

	Total	Credit card fraud	Online consumer fraud	Malware	Hacking	Online threat
I will solve it myself	101 (29.1%)	14 (42.4%)	15 (17.6%)	33 (31.4%)	31 (43.7%)	8 (15.1%)
It is not that important	33 (9.5%)	1 (3.0%)	10 (11.8%)	5 (4.8%)	4 (5.6%)	13 (24.5%)
It takes too much effort	36 (10.4%)	3 (9.1%)	17 (20.0%)	8 (7.6%)	7 (9.9%)	1 (1.9%)
There is no point, the police will not do anything about it	112 (32.3%)	10 (30.3%)	31 (36.5%)	37 (35.2%)	16 (22.5%)	18 (34.0%)
The police does not have the knowledge to tackle this type of crime	5 (1.4%)	0 (0.0%)	0 (0.0%)	3 (2.9%)	0 (0.0%)	2 (3.8%)
The police is not responsible for solving this type of crime	15 (4.3%)	0 (0.0%)	3 (3.5%)	7 (6.7%)	4 (5.6%)	1 (1.9%)
I have little confidence in the police	10 (2.9%)	0 (0.0%)	3 (3.5%)	4 (3.8%)	2 (2.8%)	1 (1.9%)
I am afraid the perpetrator will take revenge	3 (0.9%)	1 (3.0%)	0 (0.0%)	(0.0%)	1 (1.4%)	1 (1.9%)
I am ashamed that I fell victim to the crime	3 (0.9%)	0 (0.0%)	0 (0.0%)	2 (1.9%)	1 (1.4%)	0 (0.0%)
I think it is actually my own fault	13 (3.7%)	0 (0.0%)	4 (4.7%)	5 (4.8%)	3 (4.2%)	1 (1.9%)
Other	16 (4.6%)	4 (12.1%)	2 (2.4%)	1 (1.0%)	2 (2.8%)	7 (13.2%)
Total	347 (100%)	33 (100%)	85 (100%)	105 (100%)	71 (100%)	53 (100%)

computer problems myself" (44.7 percent), and (3) "I can use Linux and most other software programs and I can solve most computer problems myself" (10.9 percent).

Self-reported victimization

In addition to the experimental vignette study, respondents were also asked to self-report their victimization of 10 types of cybercrimes (see Figure 2 for offense types)[3]. In total, 303 respondents (50.9 percent) reported to have ever been a victim of 590 cybercrimes. The most prevalent types of cybercrimes were phishing (25.3 percent), malware (24.4 percent), and online consumer fraud (15.3 percent). For each type of cybercrime that victims had experienced, they were asked whether they reported the last incident to the police and/or to other organizations. In case the victim had never reported the cybercrime victimization to the police, they were asked what the most important motive was for not reporting their most recent incident to the police. If the victim had reported a cybercrime to the police at least once, they were asked for the most important motive to report the cybercrime.

Logistic regression analyses were used to examine the associations between reporting behavior and victim characteristics, since reporting to the police and reporting to other organizations were operationalized as binary variables. As a respondent could have been a victim of multiple types of cybercrime, robust standard errors were again calculated to control for this clustering.

Results

Vignette study

First, the respondents' intentions to report cybercrime victimization to the police and other organizations were analyzed using the vignette study. Across all vignettes, almost two-thirds of the respondents (65.4 percent scored 4 or 5) indicated that they would report the cybercrime in the vignette to the police, while only 19.4 percent of them would not report their victimization to the police (score 1 or 2). Moreover, more than half of the respondents (56.9 percent scored 4 or 5) (also) had the intention to report the cybercrime to other organizations than the police, while 22.9 percent indicated that they would not do that (score 1 or 2). The most often mentioned organizations to which the respondents would report were banks, credit card companies, online market places, and help desks.

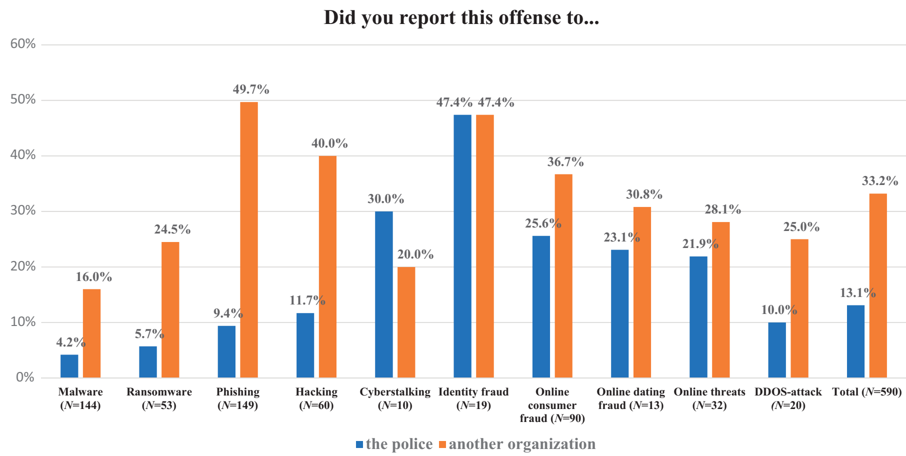

Figure 2.
Reporting rates cybercrime victimization

Table I shows the results of the ordinal logistic regression analyses in which these intentions of respondents to report cybercrime victimization to the police (Model 1) and other organizations (Model 2) were predicted. Since all 595 respondents answered three vignettes, the total sample size is 1,785. The results in Model 1 show that the type of crime influenced respondents' hypothetical reporting rates. They were significantly more likely to report victimization to the police in case of credit card fraud compared to the four other types of cybercrime. The seriousness of the offenses also significantly increased the respondents' willingness to report cybercrime to the police (OR $= 2.86$, $p < 0.01$). Moreover, if the perpetrator of the cybercrime is someone that the victim personally knows, they were significantly less willing to report victimization to the police compared to when the perpetrator is unknown (OR $= 0.74$, $p < 0.01$). No effect was found for the number of possibilities to report victimization to the police.

Most demographic variables did not predict the reporting of cybercrime victimization to the police: no significant associations were found for gender, marital status, parenthood, education, employment status, and income. Only age was significantly associated with reporting intentions. Older sample members more often intended to report their victimization to the police than younger sample members (OR $= 1.02$, $p < 0.001$). Moreover, significant associations were found for previous cybercrime victimization and subsequent reporting behavior. Those who had been a victim of cybercrime before but had never reported this to the police were less willing to report the cybercrimes from the vignettes to the police than those who had never been victim before (OR $= 0.73$, $p < 0.05$). Former cybercrime victims who had ever reported their victimization to the police, on the other hand, were more willing to report the cybercrimes from the vignettes to the police than the nonvictims (OR $= 1.65$, $p < 0.01$). Attitudes toward the police (OR $= 1.17$, $p < 0.01$) and fear for cybercrime victimization (OR $= 1.19$, $p < 0.05$) were also both significantly and positively associated with willingness to report cybercrime victimization to the police. Finally, no significant association was found between respondents' IT skill level and the intention to report cybercrime victimization to the police.

Model 2 of Table I shows the ordinal logistic regression model in which intentions to report cybercrime victimization to other organizations than the police were predicted. In line with the previous results on hypothetical crime reporting to the police, crime type influenced intended reporting rates to other organizations. Respondents indicated that they were more likely to report victimization of credit card fraud to other organizations than victimization of malware, hacking, and online threats. Similar to the results in Model 1, the seriousness of the offenses was significantly related to a higher likelihood of reporting victimization to other organizations (OR $= 1.36$, $p < 0.001$) and offenses committed by someone that the victim knows were significantly less often reported (OR $= 0.57$, $p < 0.001$).

Gender and age were the only two demographic variables that were significantly related to reporting victimization to other organizations. Women (OR $= 1.52$, $p < 0.01$) and older respondents (OR $= 1.02$, $p < 0.001$) were more likely to report to other organizations than men and younger respondents. No significant associations were found for marital status, parenthood, educational level, employment status, and income. Moreover, respondents who were the victims of cybercrime before were more likely to report victimization to other organizations, regardless of whether they had reported their previous victimization to the police (OR $= 1.80$, $p < 0.05$) or not (OR $= 1.38$, $p < 0.05$). Finally, also respondents with a higher IT skill level were more likely to report cybercrime victimization to other organizations (OR $= 1.25$, $p < 0.05$), while no significant association was found with attitudes toward the police and fear for cybercrime victimization.

Table II shows the most important motives that the respondents choose to report victimization to the police. Overall, the most often reported motives were "I want the perpetrator to be caught" (37.5 percent) and "To prevent the perpetrator from doing this again to someone else" (27.6 percent). These were also the two most reported motives for all specific types of cybercrime, except for online threats. For this type of crime, the motive "To prevent this from happening to me again" was chosen relatively often (20.8 percent). In addition, "To create a safer online environment" was relatively often reported as the most important motive to report to the police after malware (14.8 percent) and hacking (13.1 percent) victimization. "To get the damage compensated" was relatively often chosen by respondents who read the vignettes on credit card fraud (15.8 percent) and online consumer fraud (11.5 percent). Finally, "It is my duty to report crime" was seldom reported as the most important motive.

Next, Table III shows the motives of respondents who indicated that they would not report the cybercrime to the police. In total, the motives "I will solve it myself" (29.1 percent) and "There is no point, the police will not do anything about it" (32.3 percent) were most often chosen. These were also the two most reported motives to not report credit card fraud, malware, and hacking to the police. Respondents who indicated that they would not report online threats to the police relatively often chose "It is not that important" (24.5 percent) as a motive, while "It takes too much effort" (20.0 percent) was relatively often chosen to not report online consumer fraud to the police. The other motives in Table III were seldom chosen by respondents who indicated that they would not report their victimization to the police.

Self-reported victimization

Second, the actual crime reporting behavior of respondents was examined using self-reported data of the 303 respondents who indicated that they had ever been the victim of a cybercrime. Since they could report victimization of multiple types of cybercrime, a total of 590 offenses were analyzed. Figure 2 shows that, overall, 13.1 percent of these offenses were reported to the police, while 33.2 percent were (also) reported to another organization. Cyberstalking (30 percent) and identity fraud (47.4 percent) were the types of offenses that were most often reported to the police, while victims of malware infection (4.2 percent) and ransomware (5.7 percent) seldom go to the police. Figure 2 further shows that victims of phishing (49.7 percent) and identity fraud (47.4 percent) most often reported the cybercrime to other organizations, while victims of malware (16 percent) and cyberstalking (20 percent) were the least likely to do this. However, as some types of cybercrime victimization were rare, some of the results in Figure 2 are based on low sample sizes and should be interpreted with some caution.

Table IV shows the results of the logistic regression analyses in which it was predicted whether they reported this victimization to the police (Model 1) or to other organizations (Model 2). In both models, the type of cybercrime was significantly associated with reporting cybercrime victimization. The results in Model 1 show that malware infection is less often reported to the police than identity fraud (OR: 28.50, $p < 0.001$), online consumer fraud (OR: 9.58, $p < 0.001$), online threats (OR: 7.77, $p < 0.001$), cyberstalking (OR: 6.55, $p < 0.05$), online dating fraud (OR: 6.36, $p < 0.05$), and hacking (OR: 3.13, $p < 0.05$). Moreover, respondents with a higher IT skill level were more likely to report their victimization to the police (OR: 1.82, $p < 0.05$). Model 2 shows that victims of identity fraud (OR: 7.24, $p < 0.001$), phishing (OR: 5.10, $p < 0.001$), online consumer fraud (OR: 3.82, $p < 0.001$), and hacking (OR: 3.63, $p < 0.001$) were significantly more likely to report their victimization to other organizations than victims of malware. None of the other independent variables in Model 2 were significantly associated with cybercrime reporting behaviors.

The 54 respondents who indicated that they had reported cybercrime victimization to the police at least once were then asked about their motives to report the last case of victimization (see Table V). In line with the results from the vignette study (see Table II), the most reported motives were "I want the perpetrator to be caught" (27.8 percent) and "to prevent the perpetrator from doing this again to someone else" (20.4 percent). Moreover, the 278 cybercrime victims who had at least once not reported a cybercrime to the police were asked about their motives as well. Again, the two most reported motives were the same as in the

Table IV.
Logistic regression analyses reporting victimization

	Model 1: Reporting to the police			Model 2: Reporting to other organizations		
	B	Robust S.E.	Odds ratio	B	Robust S.E.	Odds ratio
Type of crime:						
Malware	(ref.)			(ref.)		
Ransomware	0.38	0.66	1.46	0.52	0.30	1.68
Phishing	0.84	0.49	2.32	1.63***	0.25	5.10
Hacking	1.14*	0.55	3.13	1.29***	0.34	3.63
Cyberstalking	1.88*	0.87	6.55	−0.23	0.88	0.79
Identity fraud	3.35***	0.62	28.50	1.98***	0.58	7.24
Online consumer fraud	2.26***	0.47	9.58	1.34***	0.32	3.82
Online dating fraud	1.85*	0.90	6.36	1.02	0.54	2.77
Online threats	2.05***	0.57	7.77	0.84	0.45	2.32
DDOS attack	1.07	0.77	2.92	0.71	0.61	2.03
Gender (male = ref.)	0.50	0.37	1.65	0.56	0.29	1.75
Age	−0.00	0.02	1.00	0.01	0.01	1.01
Marital status:						
Single	(ref.)			(ref.)		
Relationship, living together	−0.16	0.47	0.85	0.29	0.36	1.34
Relationship, not living together	0.00	0.53	1.00	0.11	0.42	1.12
Widow	0.42	0.91	1.52	0.69	0.70	1.99
Children:						
No	(ref.)			(ref.)		
Yes, not living at home	0.42	0.43	1.52	0.09	0.33	1.09
Yes, living at home	−0.05	0.48	0.95	−0.08	0.36	0.92
Education	−0.09	0.15	0.91	−0.13	0.10	0.88
Employment status:						
Employed	(ref.)			(ref.)		
Unemployed/studying	−0.25	0.46	0.78	−0.32	0.42	0.73
Pensioned	0.41	0.42	1.51	0.57	0.35	1.77
Income	−0.07	0.14	0.93	0.05	0.07	1.05
Attitudes toward police	−0.24	0.20	0.79	−0.06	0.13	0.94
Fear for cybercrime victimization	0.29	0.17	1.34	0.09	0.14	1.09
IT skill level	0.60*	0.25	1.82	0.11	0.20	1.12
N offenses	590			590		
N respondents	303			303		
Pseudo R2			0.157			0.113

vignette study: "There is no point, the police will not do anything about it" (29.1 percent) and "I will solve it myself" (21.9 percent).

Finally, the 54 respondents who had ever reported cybercrime to the police were also asked about their most recent experiences. Most of them reported their cybercrime victimization at the police station (43.4 percent) or on the Internet (37.7 percent), while only few reported to the police on the phone (18.9 percent). Only 15 respondents (27.8 percent) were satisfied or very satisfied with the way in which the police handled their report. Almost half of the reporting victims (48.1 percent), on the other hand, were (very) unsatisfied with the police after reporting their victimization. Among the victims who were unsatisfied with the way the police handled their report, the most mentioned reasons for this dissatisfaction were that the problems were not solved (46.2 percent) and that the police were indifferent (42.3 percent).

Motives to report cybercrime		Motives to not report cybercrime	
To prevent this from happening to me again	3 (5.6%)	I will solve it myself	61 (21.9%)
To prevent the perpetrator from doing this again to someone else	11 (20.4%)	It is not that important	27 (9.7%)
I want the perpetrator to be caught	15 (27.8%)	It takes too much effort	21 (7.6%)
To create a safer online environment	8 (14.8%)	There is no point, the police will not do anything about it	81 (29.1%)
It is my duty to report crime	5 (9.3%)	The police does not have the knowledge to tackle this type of crime	5 (1.8%)
To get the damage compensated	9 (16.7%)	The police is not responsible for solving this type of crime	13 (4.7%)
Other	3 (5.6%)	I have little confidence in the police	4 (1.4%)
		I am afraid the perpetrator will take revenge	1 (0.4%)
		I am ashamed that I fell victim to the crime	4 (1.4%)
		I think it is actually my own fault	10 (3.6%)
		Other	51 (18.3%)
Total	54 (100%)	Total	278 (100%)

Table V. Motives to (not) report cybercrime

Conclusion and discussion

In this study, we used a sample of 595 Dutch citizens to examine their intended reporting behavior and their actual reporting behavior after cybercrime victimization. Determinants of both reporting to the police as well as to other organizations were examined, while we also studied motivations to report a crime to the police or not and past experiences with reporting cybercrime victimization to the police.

Results from both the vignette study and the self-report study show that the type of cybercrime predicts reporting victimization to the police, although not all comparisons were significant. A distinction between cyber-enabled crimes (i.e. traditional crimes committed through the use of IT but not aimed at IT) and cyber-dependent crimes (i.e. new types of crime committed through the use of IT and also aimed at IT) was visible. Victims of various forms of online fraud (e.g. online consumer fraud, online dating fraud, and identity fraud), crimes that are most likely to be associated with financial loss, were more likely to report their victimization to the police than victims of malware. Similarly, the vignette study also found that the respondents were most likely to report credit card fraud to the police. Actual victimization of interpersonal cybercrimes, such as cyberstalking and online threats, was also more often reported to the police than malware. Similar results were found in previous studies, which showed higher reporting rates for online fraud than hacking (e.g. van der Weijer *et al.*, 2018; CBS, 2018a). These results suggest that victims might think that the police are not responsible for solving these cyber-dependent crimes, but this was seldom mentioned as the most important reason to not report the crime to the police. Instead, respondents most often stated that they did not report the crime to the police because they will solve it themselves or because the police will not do anything about it. Although the police indeed do not have the capacity to investigate each malware infection or phishing email, it is still important for the police to have information about the rates and trends of these types of cybercrime victimization.

In the vignette study, also several other determinants of cybercrime reporting were found. In line with several studies on reporting of traditional crimes (e.g. Baumer and Lauritsen, 2010; Estienne and Morabito, 2016; Goudriaan *et al.*, 2005; Kääriäinen and Sirén, 2011), it was found that more serious offenses were more often reported to the police and other organizations than less serious offenses. Another factor of influence was the victim–offender relationship. The vignette results demonstrated that offenses would be less often reported in situations where the victim personally knows the perpetrator compared to when the identity of the perpetrator is unknown. This finding that a known perpetrator reduces the likelihood of reporting is also found in traditional crimes (e.g. Tolsma *et al.*, 2012). Reducing the time investment of reporting by providing more possibilities to report victimization to the police (e.g. on the phone or the Internet) did not increase respondents' intentions to report cybercrime victimization to the police. The same result was found in a previous study among a Dutch student sample (Jong *et al.*, 2018) and, thus, suggests that reporting rates will not increase by simply offering more possibilities to report cybercrime to the police.

We did not find many significant associations between demographic characteristics and reporting behaviors. In the vignette study, only older respondents were more likely to report victimization to the police and to other organizations, while women more often intended to report victimization to other organizations than men. In the self-report study with actual cybercrime victims, none of the demographics were related to the reporting of cybercrime victimization to either the police or other organizations. This is remarkable, as in a previous study on cybercrime reporting in the Netherlands, several significant results were found between demographics and reporting behavior in a large cross-sectional Dutch population survey (van der Weijer *et al.*, 2018). Within their cybercrime sample, they found that factors such as age, gender, nationality, marital status, and occupational status influenced reporting rates. Possibly our results are different because van der Weijer *et al.*, 2018 only examined three types of cybercrime (i.e. identity theft, online consumer fraud, and hacking) while in the current study many more types of cybercrime were included. Another possible explanation is that the larger sample size (N = 36,261) in the study of van der Weijer *et al.*, 2018 made it possible to find significant results, even when associations were weak. Nonetheless, the explained variance in their analysis (pseudo $R^2 = 0.083$) was considerably lower than in the current study (pseudo $R^2 = 0.157$), which suggests that those significant demographic variables in the study of van der Weijer *et al.*, 2018 probably did not explain cybercrime reporting to the police very well. This limited role of demographics in explaining reporting behaviors suggests that it is not possible to make a profile of cybercrime victims that do not report their victimization. Interventions or campaigns to increase reporting rates, therefore, should be targeted on a general public, rather than on a specific demographic group.

The results of the vignette study further show that those who are more afraid to become a victim of cybercrime and have more positive attitudes toward the police are more likely to report cybercrime victimization. Also, respondents who had reported a cybercrime to the police in the past had more intentions to report victimization to the police. This latter finding is remarkable given that almost half of the victims were (very) dissatisfied with the way the police handled their report, mostly because the problem was not solved and because the police reacted indifferently. In line with this finding, "the police will not do anything about it" was, overall, most often chosen as the motive to not report cybercrime victimization to the police. Police dissatisfaction was also reported in previous studies in which it was described how victims who wanted to report their cybercrime victimization were simply sent away at the police station (Cross *et al.*, 2016; Leukfeldt *et al.*, 2018, 2019) and which show that the organization of the police is not well equipped to deal with cybercrime (Bossler *et al.*, 2019). As it is important for victims to tell their story (Cross *et al.*, 2016; Leukfeldt *et al.*, 2018), it is important that the police take victims of cybercrime seriously and not act indifferently when they report their victimization.

Another interesting finding of this paper concerns the large discrepancy between the intentions of the respondents to report cybercrimes to the police in the vignette study and their actual reporting behaviors after real cybercrime victimization. Almost two-thirds of the respondents indicated to report the cybercrimes in the vignettes, while only 13 percent of the victims actually made a report to the police. These results suggest that vignettes may not be the most appropriate way to study crime reporting and indicate that the results from the vignette study should be interpreted with some caution. There are several possible explanations for this discrepancy between intended and actual reporting. First, this difference may have been caused by the type and seriousness of the tested crimes. It is possible that the hypothetical situations in our vignettes described more serious cases of cybercrime than most of the cybercrime incidents in real life. A second, and more likely, explanation is that police reporting may be subjected to the intention–behavior gap. In short, people do not always do the things that they intend to do (Sheeran and Webb, 2016). This phenomenon is widespread and prevents people from living a healthier lifestyle (De Bruin *et al.*, 2012), quit smoking (Kovač and Rise, 2007), behave in an environmentally friendly manner (Kollmuss and Agyeman, 2002), and handle our privacy better (Aqcuisti *et al.*, 2015). In a meta-analysis of 10 meta-analyses on the intention–behavior relationship, Sheeran (2002) found that only 28 percent of behavior could be explained by people's intentions, which means that three-quarters of our behavior is determined by other factors. Luckily, a lot of studies have investigated which factors influence the intention–behavior gap and how this gap can be closed. Promising avenues include if–then plans and progress monitoring interventions (Sheeran and Webb, 2016). Future research could investigate which of these interventions are most suitable for the context of crime reporting to the police.

Finally, it could be effective if the police actively work together with other relevant public and private organizations, such as banks, credit card companies, online market places, and help desks. As our results show that victims of most types of cybercrime more often reported victimization to such organizations rather than to the police, this could help the police to gain insights in the prevalence and trends of these cybercrimes. Over the past couple of years, we have already seen such partnerships in the Netherlands. For example, the police, the largest online market place, and financial institutions are cooperating in a National Hotline for Internet Scams. There is also an Electronic Crimes Taskforce, in which a team of employees of financial institutions and police officers work together to prepare cases. The effectiveness of such collaborations should be examined in future research in order that they can be strengthened and, if effective, other countries where such collaborations do not yet exist can set them up.

Notes

1. The original sample included 604 individuals, but nine respondents were excluded from the analytic sample because they finished the questionnaire in 3 min or less. This was deemed too short to have seriously answered all the questions as the median duration of the survey was 10 min, with a mean of 41 min and a standard deviation of 362 min. This large standard deviation is the consequence of 12 respondents who took more than 100 min (with a maximum of 7416 min) to finish the questionnaire. These 12 respondents were not excluded, as it was possible to take a break and continue at a later moment to finish the questionnaire.
2. The VIF values in all regression analyses were lower than 4, indicating that there was no multicollinearity between the independent variables.
3. The respondents were only shown the title of the types of cybercrimes, without a description.

References

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015), "Privacy and human behavior in the age of information", *Science*, Vol. 347 No. 6221, pp. 509-514.

Baumer, E.P. and Lauritsen, J.L. (2010), “Reporting crime to the police, 1973-2005: a multivariate analysis of long-term trends in the national crime survey (NCS) and national crime victimization survey (NCVS)”, *Criminology*, Vol. 48 No. 1, pp. 131-185.

Bidgoli, M. (2015), *A Mixed Methods Approach to Understanding Undergraduate Students' Victimization, Perceptions, and Reporting of Cybercrime*, University of California, Irvine.

Bossler, A., Holt, T.J., Cross, C. and Burruss, G.W. (2019), “Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness”, *Security Journal*, doi: 10.1057/s41284-019-00187-5.

De Bruin, M., Sheeran, P., Kok, G., Hiemstra, A., Prins, J.M., Hospers, H.J. and van Breukelen, G.J. (2012), “Self-regulatory processes mediate the intention–behavior relation for adherence and exercise behaviors”, *Health Psychology*, Vol. 31 No. 6, pp. 695-703, doi: 10.1037/a0027425.

Burgard, A. and Schlembach, C. (2013), “Frames of fraud: a qualitative analysis of the structure and process of victimization on the Internet”, *International Journal of Cyber Criminology*, Vol. 7 No. 2, p. 112.

CBS (2018a), *Veiligheidsmonitor 2017. Den Haag/Heerlen/Bonaire*, Den Haag: Centraal Bureau voor de Statistiek.

CBS (2018b), “Trends in Nederland 2018”, available at: https://longreads.cbs.nl/trends18/maatschappij/cijfers/onderwijs.

CBS (2019), “CBS statline”, available at: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/37296ned/table?ts=1571893768002.

Cross, C.A., Richards, K.M. and Smith, R., (2016), “The reporting experiences and support needs of victims of online fraud”, *Trends and Issues in Crime and Criminal Justice*, Canberra: Australian Institute of Criminology, Vol. 518 pp. 1-14, available at: https://aic.gov.au/publications/tandi/tandi518.

Domenie, M.M.L., Leukfeldt, E.R., van Wilsem, J.A. Jansen, J. and Stol, W.Ph (2013), *Victimisation in a Digitised Society*, Eleven International Publishing, Den Haag.

Estienne, E. and Morabito, M. (2016), “Understanding differences in crime reporting practices: a comparative approach”, *International Journal of Comparative and Applied Criminal Justice*, Vol. 40 No. 2, pp. 123-143, doi: 10.1080/01924036.2015.1086397.

Goudriaan, H. and Nieuwbeerta, P. (2007), “Contextual determinants of juveniles' willingness to report crimes. A vignette experiment”, *Journal of Experimental Criminology*, Vol. 3 No. 2, pp. 89-111.

Goudriaan, H., Lynch, J.P. and Nieuwbeerta, P. (2004), “Reporting to the police in western nations: a theoretical analysis of the effects of social context”, *Justice Quarterly*, Vol. 21 No. 4, pp. 933-969.

Goudriaan, H., Nieuwbeerta, P. and Wittebrood, K. (2005), “Overzicht van onderzoek naar determinanten van aangifte doen bij de politie. Theorieën, empirische bevindingen, tekortkomingen en aanbevelingen”, *Tijdschrift voor Veiligheid*, Vol. 4 No. 1, pp. 27-48.

Goudriaan, H., Wittebrood, K. and Nieuwbeerta, P. (2006), “Neighbourhood characteristics and reporting crime effects of social cohesion, confidence in police effectiveness and socio-economic disadvantage”, *British Journal of Criminology*, Vol. 46 No. 4, pp. 719-742.

Gutierrez, C.M. and Kirk, D.S. (2017), “Silence speaks: the relationship between immigration and the underreporting of crime”, *Crime and Delinquency*, Vol. 63 No. 8, pp. 926-950.

Guzy, N. and Hirtenlehner, H. (2015), “Trust in the German police: determinants and consequences for reporting behavior”, in Meško, G. and Tankebe, J. (Eds), *Trust and Legitimacy in Criminal Justice*, Springer, Cham, pp. 203-229.

Holt, T.J. and Bossler, A.M. (2008), “Examining the applicability of lifestyle-routine activities theory for cybercrime victimization”, *Deviant Behavior*, Vol. 30 No. 1, pp. 1-25.

Jansen, J. and Leukfeldt, E.R. (2018), “Coping with cybercrime victimization: an exploratory study into impact and change”, *Journal of Qualitative Criminal Justice and Criminology*, Vol. 6 No. 2, pp. 205-228.

Jong, L., Leukfeldt, E.R. and van de Weijer, S. (2018), “Aangiftebereidheid na slachtofferschap van cybercrime”, *Tijdschrift voor Veiligheid*, Vol. 17 Nos 1-2, pp. 66-78.

Kääriäinen, J. and Sirén, R. (2011) ,"Trust in the police, generalized trust and reporting crime", *European Journal of Criminology*, Vol. 8 No. 1, pp. 65-81.

Kollmuss, A. and Agyeman, J. (2002), "Mind the Gap: why do people act environmentally and what are the barriers to pro-environmental behavior?", *Environmental Education Research*, Vol. 8 No. 3, pp. 239-260, doi: 10.1080/13504620220145401.

Kovač, V.B. and Rise, J. (2007), "The relation between past behavior, intention, planning, and quitting smoking: the moderating effect of future orientation", *Journal of Applied Biobehavioral Research*, Vol. 12 No. 2, pp. 82-100, doi: 10.1111/j.1751-9861.2007.00015.x.

Leukfeldt, E.R., Notté, R.J. and Malsch, M. (2018), *Slachtofferschap van online criminaliteit. Een onderzoek naar behoeften, gevolgen en verantwoordlijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*, Den Haag: Ministerie van Justitie en Veiligheid.

Leukfeldt, E.R., Notté, R.J. and Malsch, M. (2019), "Exploring the needs of victims of cyber-dependent and cyber-enabled crimes", *Victims and Offender*, Vol. 15 No. 1, pp. 1-18.

ONS (2016), *Crime in England and Wales: Year Ending December 2015*, ONS, London.

Schnebly, S.M. (2008), "The influence of community-oriented policing on crime-reporting behavior", *Justice Quarterly*, Vol. 25 No. 2, pp. 223-251.

Sheeran, P. (2002), "Intention—behavior relations: a conceptual and empirical review", *European Review of Social Psychology*, Vol. 12 No. 1, pp. 1-36, doi: 10.1080/14792772143000003.

Sheeran, P. and Webb, T.L. (2016), "The intention-behavior gap", *Social and Personality Psychology Compass*, Vol. 10 No. 9, pp. 503-518, doi: 10.1111/spc3.12265.

Slocum, L.E.E., Taylor, T.J., Brick, B.T. and Esbensen, F.A. (2010), "Neighborhood structural characteristics, individual-level attitudes, and youths' crime reporting intentions", *Criminology*, Vol. 48 No. 4, pp. 1063-1100.

Tarling, R. and Morris, K. (2010), "Reporting crime to the police", *British Journal of Criminology*, Vol. 50, pp. 474-490, doi: 10.1093/bjc/azq011.

Tolsma, J., Blaauw, J. and Te Grotenhuis, M. (2012), "When do people report crime to the police? Results from a factorial survey design in The Netherlands, 2010", *Journal of Experimental Criminology*, Vol. 8 No. 2, pp. 117-134.

Veenstra, S., Zuurveen, R. and Stol, W.Ph. (2015), *Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen zonder Personeel in Nederland*, Leeuwarden: Lectoraat Cybersafety.

van der Weijer, S., Leukfeldt, E.R. and Bernasco, W. (2018), "Reporting crime to the police: a comparison between traditional crime and cybercrime", *European Journal of Criminology*, Vol. 16 No. 4, pp. 486-508, doi: 10.1177/1477370818773610.

van der Weijer, S., Leukfeldt, E.R. and van der Zee, S. (2020), "Slachtoffer van cybercriminaliteit, wat nu? Een onderzoek naar aangiftebereidheid onder burgers en mkb'ers", victim of a cybercrime, now that?, *A Study into Willingness to Report Cybercrime Amongst Civilians and Organizations*, SDU publishing, Den Haag.

van't Hoff-de Goede, S., van der Kleij, R., van de Weijer, S. and Leukfeldt, R. (2019), *Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie, en online gedrag van Nederlanders*, WODC, The Hague.

Appendix

Table. AI.
Items used to measure attitudes toward the police

Items	Factor loadings
The police know how to catch criminals.	0.7347
The police want to be in contact with citizens.	0.8109
The police take into account the wishes of society.	0.8014
The police work well with the residents.	0.8246
If it really matters, then the police are there for you.	0.7925
The police are easy to approach.	0.6341
The police inform the citizens.	0.7378
The police are successfully fighting crime.	0.6715
If it really matters, the police will do their utmost to help you.	0.7211

Table AII.
Items used to measure fear for cybercrime victimization

Items	Factor loadings
I am scared of becoming a victim of cybercrime in the near future.	0.6895
The idea that someone can log into my online bank account without permission scares me.	0.7414
I am concerned that I can become a victim of phishing.	0.7800
I am concerned about the possibility that my computer can be hacked.	0.8246
I think it can easily happen that I get scammed online.	0.5201
The fact that I can get ransomware on my computer worries me.	0.8170
It is quite possible that I will become a victim of cybercrime in the coming year.	0.4911
If I became a victim of cybercrime, it could have serious consequences.	0.5131

Corresponding author
Rutger Leukfeldt can be contacted at: RLeukfeldt@nscr.nl