Computers & Security 139 (2024) 103693

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Cybercrime during the COVID-19 pandemic: Prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands

Steve van de Weijer [a,*], Rutger Leukfeldt [a,b,c], Asier Moneva [a,b]

[a] Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), the Netherlands
[b] Centre of Expertise Cyber Security, The Hague University of Applied Sciences, the Netherlands
[c] Faculty of Law and Faculty of Governance and Global Affairs, Leiden University, the Netherlands

ARTICLE INFO

Keywords:
Cybercrime
Online crime
Internet
Remote work
Businesses
Victimization
COVID-19
Pandemic
coronavirus

ABSTRACT

The outbreak of the COVID-19 virus in December 2019 and the restrictive measures that were implemented to slow down the spread of the virus have had a significant impact on our way of life. The sudden shift from offline to online activities and work may have resulted in new cybersecurity risks. The present study therefore examined changes in the prevalence, nature and impact of cybercrime among Dutch citizens and SME owners, during the pandemic. Qualitative interviews with ten experts working at various public and private organizations in the Netherlands that have insights into cybercrime victimization and data from victim surveys administrated in 2019 and 2021 were analyzed. The results show that there was only a small, non-statistically significant increase in the prevalence of cybercrime during the pandemic among citizens and SME owners. Nevertheless, the COVID-19 pandemic did have an impact on the modus operandi of cybercriminals: victims indicated that a considerable proportion of the offenses was related to the COVID-19 pandemic, particularly in the case of online fraud. Moreover, the use of new applications and programs for work was associated with an increased risk of cybercrime victimization during the COVID-19 crisis. These results suggest that increases in rates of registered cybercrime that were found in previous studies might be the consequence of a reporting effect and that cybercriminals adapt their modus operandi to current societal developments.

1. Introduction

The outbreak of the COVID-19 virus in December 2019 in the Chinese city of Wuhan has had a significant impact on the way of life worldwide. In almost all countries restrictive measures were implemented to slow down the spread of the virus, including travel restrictions, social distancing, the closing of companies and public buildings, curfews and lockdowns. Naturally, these measures have had a significant influence on our way of life and it is for example likely that never before have so many people worked from home simultaneously as during the COVID-19 pandemic. These changes in our lives were expected to also lead to changes in crime rates (Stickle and Felson, 2020). This article will focus on the impact of the pandemic on cybercrime victimization in the Netherlands.

The first case of a COVID-19 infection in the Netherlands was confirmed on 27 February 2020, after which the number of infections quickly increased. In order to limit the further spread of the virus as much as possible, various freedom-restricting measures were implemented in the Netherlands, as in almost all other countries. From 23 March 2020 to 1 May 2020, a series of restrictions were implemented in the Netherlands and people were asked to maintain distance from each other, stay at home and work as much as possible, and schools, sports clubs, bars, restaurants, and shops were closed. In the Netherlands, this period was also referred to as an "intelligent lockdown". In the two years following this "intelligent lockdown", there were periods of scaling up and scaling down these restrictions. The strictest restrictions were implemented during two "hard lockdowns" in December 2020 and December 2021.[1]

In the first year of the pandemic, the number of registered crimes in the Netherlands was approximately 6 percent lower than in the same period the previous year, with the largest differences observed during the periods with the strictest measures (i.e., the "intelligent lockdown"

* Corresponding author.
E-mail address: svandeweijer@nscr.nl (S. van de Weijer).

[1] See https://www.rivm.nl/en/coronavirus-covid-19/current-information/archive-covid-19-updates for a detailed timeline of the pandemic and measures against the spread of COVID-19 in the Netherlands.

https://doi.org/10.1016/j.cose.2023.103693
Received 2 August 2023; Received in revised form 19 December 2023; Accepted 26 December 2023
Available online 27 December 2023

and “hard lockdown”). This decrease was particularly evident in crimes that are typically committed when the victim is not at home, such as residential burglary, pickpocketing, and bicycle theft (Kruisbergen et al., 2021). For domestic violence, which typically occurs at home or in the household, there were also concerns about an increase, although this was not found in official reports (Coomans et al., 2022).

In addition to these traditional crimes, several experts have also pointed out the cybersecurity risks of remote work (e.g., Georgiadou et al., 2022). This is particularly relevant for small and medium-sized enterprises (SMEs) because SMEs are the backbone of the Dutch economy (accounting for 63 % of the Gross Domestic Product, 71 % of employment, and a total revenue of 1023 billion euros; Staat van het MKB, 2021), while we also know that this group of companies is relatively often targeted by cyberattacks and has limited resources to defend themselves against them (Moneva and Leukfeldt, 2023; Notte et al., 2019; Veenstra et al., 2015). At the same time, SMEs are likely not well-equipped to support remote working on a large scale (Bada and Nurse, 2019), and have therefore had to improvise hastily to enable remote work.

Therefore, this study examines to what extent the outbreak of the COVID-19 virus and the implemented restrictions during the pandemic have led to more cyber insecurity for both citizens and SMEs, and what lessons we can learn from this for the future. We examine the prevalence, nature and impact of online threats and incidents. This provides insights into how sudden shifts from offline to online activities result in new cybersecurity risks (e.g., Buil-Gil et al., 2021a; Kemp et al., 2021). It is crucial for SMEs to assess the measures they can and should take during crises as previous research has shown that SMEs have little insight into cyber risks and, as a result, do not know which measures they should implement (Notte et al., 2019). Additionally, SMEs often lack the resources and knowledge to effectively defend against cybercriminals (Bada and Nurse, 2019).

1.1. Literature review

The unprecedented mobility restriction policies implemented to mitigate the effects of the COVID-19 pandemic created a perfect scenario for testing criminological theories. The pandemic was even referred to as the largest criminological experiment in history (Stickle and Felson, 2020). According to the Routine Activities Approach (Cohen and Felson, 1979), the recurrent and prevalent routines of people shape criminal opportunities. During the pandemic, mobility restrictions directly affected the daily lives of people, limiting them to a large extent to their household. This produced a shift from offline to online work and leisure activities (Buil-Gil et al., 2021a), which would have resulted in a reduction of most forms of traditional crime (e.g., Nivette et al., 2021) in favor of cybercrime (Buil-Gil et al., 2021a; Kemp et al., 2021; see also Miró-Llinares and Moneva, 2019).

Much empirical research on cybercrime and COVID-19 uses time series analysis on longitudinal data on cybercrime and different forms of (online) fraud to test hypotheses based on the Routine Activities Approach. The results of all studies using Auction Fraud UK data show strong support for this theoretical framework. For example, researchers found that reports of cybercrime increased during the pandemic beyond predicted levels, especially during the most severe lockdown periods, and matching changes in mobility (Buil-Gil et al., 2021a; Buil-Gil and Zeng, 2022; Johnson and Nikolovska, 2022; Kemp et al., 2021). Yet these variations were not homogeneous for all crime types and victims. For example, it appears that while cybercrimes such as hacking and online shopping fraud increased, doorstep fraud did not (Johnson and Nikolovska, 2022), and that this increase in cybercrime has mainly affected individuals rather than organizations (Buil-Gil et al., 2021a). In the case of romance fraud, it appears that younger people were more often targeted than older people (Buil-Gil and Zeng, 2022). An analysis of data from the Police Service of North Ireland appears to confirm the overall findings and highlights that the increase in cybercrime and fraud during the pandemic "accelerated the long-term upward trend in online crime" (Buil-Gil et al., 2021b, p. 1). As mobility resumed, levels of cybercrime and online fraud bounced back a little, but remained higher than before (Johnson and Nikolovska, 2022).

Some studies provide a more global perspective on the impact of COVID-19 on cybercrime. World Health Organization (WHO) data, along with news outlets, blog posts, reports, and social media posts reveal that, after the initial outbreak, large scale cyber-attacks around the world became more frequent (Lallie et al., 2021). A thematic analysis of 185 documents provided by FraudWatch International on different records of various cyber frauds shows how the creativity of offenders adapts to the fraud opportunities and the dynamic context and generates the evolution of the pandemic (Naidoo, 2020). Along these lines, data from the US Federal Trade Commission suggest that older people suffered more economic losses than younger people and were targeted more frequently by certain types of fraud schemes such as tech support or helpdesk scams (Payne, 2020). Recent research using data from India’s National Commission for Women also suggests that there was an increase in cybercrime complaints during the lockdown imposed on 25 March 2020 (Ravindran and Shah, 2023). At the level of cybersecurity culture, a questionnaire administered to 264 critical infrastructure employees in Europe revealed that 53 percent did not receive any cybersecurity guidance during the pandemic (Georgiadou et al., 2022), which would reinforce the idea that organizations were not prepared to respond to the cybersecurity challenge posed by the situation.

Consistent with international research, an increase in registered cases of cybercrime was also found in the Netherlands during the pandemic. Kruisbergen et al. (2021) investigated changes in police registrations of cybercrime, including all forms of cybercrime and fraud with an online component (such as consumer fraud and friend-in-need fraud[2]). They found that during the first 52 weeks of the pandemic, the police registered 102,200 cases of cybercrime, compared to 62,500 in the same period the previous year. This represents a 64 percent increase, which was most pronounced during the weeks of the first lockdown, when there was a 112 percent increase in cybercrime. However, it should be noted that the upward trend in police registrations had already begun before the first lockdown.

Overall, these international and Dutch studies indicate there was an increase in registered cybercrime during the pandemic. However, studies using self-report data from victims and offenders show less consistent results. For example, a US study in which two different samples answered the same questionnaire - one before and one during the pandemic - found that the online activities and victimization of cybercrime reported by respondents did not change during the pandemic. This could, however, be the consequence of the fact that the post-COVID-19 sample was asked in April 2020 about cybercrime victimization in the past twelve months, which only included a couple of months during the pandemic (Hawdon et al., 2020). Moreover, results from the Crime Survey for England and Wales show that citizens did not report more computer viruses and bank and credit account fraud during the pandemic than prior to the pandemic, while consumer and retail fraud, advance fee fraud, and unauthorized access to personal information (including hacking) did increase during the pandemic (Jones, 2022). Moreover, results from the Cyber Security Breaches Survey show that 46 percent of UK businesses reported breaches or attacks in 2020, compared to only 32 percent in 2019. It is, however, important to note that in 2017 (46 %) and 2018 (43 %) the prevalence of breaches and

[2] Friend-in-need fraud, also known as Whatsapp fraud, is a social engineering technique in which a person receives a seemingly urgent message via WhatsApp from someone they know, such as a friend or family member, requesting a quick money transfer. The sender, however, is not the real acquaintance, but an imposter who intends to swindle money from the recipient (van‘t Hoff-de Goede & Leukfeldt, 2021).

attacks among businesses was quite similar as in 2020 (Johns and Ell, 2023). In the Netherlands, Weulen Kranenbarg and Weerman (2022) examined changes in online activities and engagement in cybercrime using a longitudinal dataset with self-reports from 289 young people (aged 13–25) in ICT education (secondary school and higher vocational education). The results of this study showed, as expected, an increase in online activities and contact with friends during the early months of the pandemic, while offline activities and contact decreased. However, the extent to which these young people engaged in cybercrime remained largely unchanged. Just before the start of the pandemic (January-February 2020), the majority of the young people reported the same level of cybercrime as during the pandemic (June 2020), with a larger percentage reporting a decrease compared to those who reported an increase. This result was consistent for almost every type of cybercrime, as well as for all traditional forms of cybercrime examined.

The discrepancy between some of the results from self-report studies and studies based on registered reports may be explained by a *reporting effect*: levels of perpetration and victimization of cybercrime have remained constant, but victims are more likely to report their victimization to the police or other agencies during the pandemic because more resources and possibilities to report are made available to them. In the Netherlands, for example, it became possible to file online reports for friend-in-need fraud starting from April 2020, which may have made it easier for victims to seek assistance from the police.

1.2. The present study

The present study adds to the existing literature on the impact of the COVID-19 pandemic on cybercrime victimization by using a mixed-methods approach, including qualitative interviews and a quantitative survey. This is the first Dutch study to examine the impact of the COVID-19 pandemic on cybercrime victimization through a victim survey. To test and deepen the insights from the literature and exploratory qualitative interviews, we administered a questionnaire about experiences with cybercrime victimization to citizens and SME owners in the Netherlands in two waves: 2019 and 2021. Moreover, unlike the cross-sectional victim surveys in previous American (Hawdon et al., 2020) and British studies (Johns and Ell, 2023; Jones, 2022), this study utilizes a panel design where the same respondents were surveyed both before and during the pandemic, eliminating potential sample differences as an explanation for any observed changes.

The following three research questions are central to this study:

1. *To what extent has the prevalence and nature of cybercrime changed during the COVID-19 pandemic?*
2. *What were the consequences of victimization by cybercrime during the COVID-19 pandemic?*
3. *Is there a relationship between changes in internet usage and victimization by cybercrime during the COVID-19 pandemic?*

2. Methods

2.1. Qualitative interviews

The aim of the qualitative interviews was to gain an initial understanding of the extent to which the nature and scope of cyber threats have changed due to the COVID-19 pandemic and to assess the prevalence, nature, and impact of cybercrime during the pandemic. We conducted interviews with ten experts working at various public and private organizations in the Netherlands that have insights into cybercrime victimization: the National Cyber Security Centre (NCSC), the Royal Association MKB-Nederland (the largest entrepreneurs' organization in the Netherlands, connecting over 120 branch organizations and 250 regional and local entrepreneurs' fellowships), the Digital Trust Centre (DTC), the Chamber of Commerce, the Police, the Fraud Helpdesk, two cybersecurity companies, and one insurance company. These companies were selected because they are involved in the fight against cybercrime in the Netherlands and have insight into cybercrime victimization. All respondents had experience with protecting organizations against cyberattacks and/or handling cybersecurity incidents. We used snowball sampling to select organizations and experts to interview. All the organizations and experts that were approached agreed to do the interview. The interviews took place between January 2021 and May 2021. All interviews were one-on-one interviews, except the interview with DTC, in which we interviewed two respondents simultaneously. All interviews were done via Microsoft Teams and lasted between 45 and 90 min. During each interview, respondents were asked about other potentially relevant organizations and experts to interview. We stopped interviewing after we reached the point of saturation. To analyze the interviews, a pre-established coding system – or procedural coding method – based on the interview protocol was used. All interviews were in Dutch, the quotes used in this article are translated from Dutch to English.

2.2. Quantitative survey

This quantitative part of this study uses data from participants from the I&O Research panel. The first round of data was collected between 2 May and 13 May 2019 for a research project that focused on cybercrime victimization among Dutch citizens and SME owners (van de Weijer et al., 2020). At that time, 2823 members of the panel were approached to participate in the research, in return for a gift voucher. Among them 1133 respondents (response rate: 40.1 %) completed the online questionnaire and answered questions about - among other things – cybercrime victimization. These respondents were divided into two groups: 529 SME owners and 604 citizens. The first group consisted of self-employed individuals or entrepreneurs with employees, while the second group comprised individuals who were employed, students, unemployed, or retired. All respondents were 18 years or older. Although the total 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 our sample as 28.8 percent was 65 years or older, while this was only 19.2 percent in the Dutch population (Statistics Netherlands, 2023). On average the sample members were 56.88 years old (std. dev.:12.89; ranging from 18 to 88 years). Second, men were overrepresented as 657 sample members are men (58.0 %) compared to 49.7 percent in the Dutch population. Third, our sample members more often had a high educational level (57.7 %) compared to the general population (30 %) in the Netherlands (Statistics Netherlands, 2018). Fourth, SME owners were overrepresented in our sample as they were deliberately oversampled in order to examine cybercrime victimization among both SME owners and other citizens.

Subsequently, between 15 April and 17 May 17 2021 – over a year after the start of the COVID-19 pandemic – we attempted to approach the same respondents from the I&O Research panel for participation in the second online questionnaire. Unfortunately, this was not possible in all cases, as some respondents were no longer part of the panel (7.8 % of SME owners and 7.7 % of citizens) or could not or did not want to participate. In total, 241 SME owners from the 2019 sample were surveyed again in 2021 (*attrition rate* = 54.4 %), and 416 citizens were surveyed in both years (*attrition rate* = 31.1 %). There were 25 cases where a respondent participated as a citizen in 2019 but had become an SME owner in 2021. The reverse situation – an SME owner in 2019 and a citizen in 2021 – occurred 54 times. To increase the sample size of the second wave, we also administered the questionnaire to respondents who did not participate in 2019. This resulted in an additional 412 SME owners and 329 citizens who only participated in 2021. The total sample in 2021 consist of 678 SME owners and 799 citizens. The average age of the sample members in 2021 was 56.73 years (std. dev.:14.16; ranging from 18 to 90 years), 56.5 percent of them were males, and 59.6 percent had a high educational level.

The sampling process is summarized in Fig. 1.

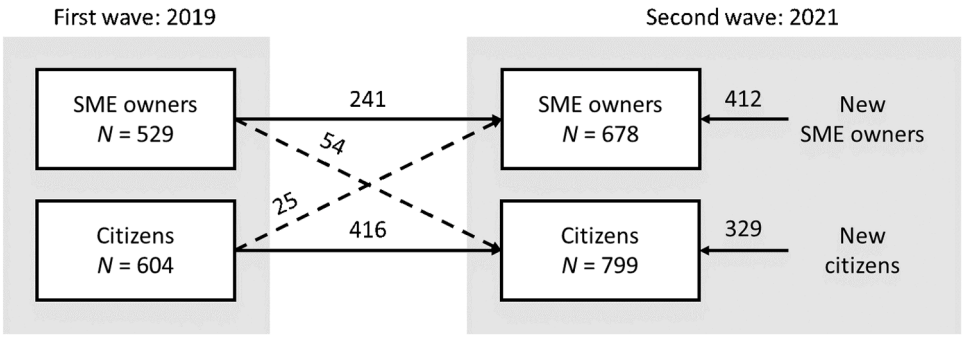

Fig. 1. Overview of the samples of SME owners and citizens in 2019 and 2021.

2.2.1. Measures

This section describes the variables used in the study. The variables related to cybercrime victimization were measured consistently across the two waves of data collection. The remaining variables used in this study were only measured in 2021, primarily because they are directly related to the COVID-19 pandemic.

Cybercrime victimization. Cybercrime victimization was measured by asking respondents in both 2019 and 2021 whether they had ever been a victim of ten types of cybercrime. These include six types of cyber-enabled crimes (i.e., traditional crimes committed through the use of IT but not aimed at IT: phishing, cyberstalking, identity fraud, consuming fraud, online dating fraud, and online threats) and four types of cyber-dependent crimes (i.e., new types of crime committed through the use of IT and also aimed at IT: malware, ransomware, hacking, and DDoS-attacks). Respondents could indicate whether this occurred in the past 12 months, occurred longer ago, or did not occur. In this study, we only differentiate between respondents who became victims in the past 12 months and those who did not. This allows us to compare the prevalence of cybercrime during the pandemic (between April/May 2020 and April/May 2021) and prior to the pandemic (between May 2018 and May 2019). For each individual type of cybercrime, a dichotomous variable was created indicating whether respondents had become victims or not. Additionally, overarching variables were created indicating whether or not respondents had been a victim of at least one type of cybercrime, one type of cyber-enabled crimes or one type of cyber-dependent crimes.

COVID-19 cybercrime victimization. In the second wave, all respondents who had been victims of a specific type of cybercrime in the last twelve months were asked whether the perpetrators had exploited the COVID-19 crisis when committing the crime. Additionally, respondents who had been victims in the last twelve months were asked to indicate how seriously they perceived the offense themselves. Respondents could choose from three response options: not very serious (1), moderately serious (2), and very serious (3). These victims were also asked whether they had suffered financial damage the last time they were victims of a specific offense, and if so, how much.

Internet usage. In the second wave, respondents were asked about changes in their internet usage during the COVID-19 pandemic through the following three questions:

- To what extent has your work-related internet usage at work (e.g., in the office, workplace, on-site with clients) increased or decreased since the outbreak of the coronavirus?
- To what extent has your work-related internet usage at home increased or decreased since the outbreak of the coronavirus?
- To what extent has your internet usage in personal time increased or decreased since the outbreak of the coronavirus?

For all three questions, respondents could answer on a 5-point scale, ranging from strongly decreased (1) to strongly increased (5), or indicate that a question was not applicable. Additionally, respondents were asked whether, for work-related activities at work and at home, they have had to use new applications or programs on their computer since the outbreak of the coronavirus.[3]

3. Results

3.1. Qualitative interviews

When asked about the key cyber threats before the outbreak of the COVID-19 virus, respondents mentioned various forms of cybercrime. The most frequently mentioned were ransomware and various types of online banking fraud (phishing, banking malware, bank helpdesk fraud). Additionally, depending on the core activities of their organization, respondents mentioned a range of other cybercrimes, including friend-in-need fraud, business email compromise (BEC) fraud, and espionage. This finding is consistent with previous studies on cybercrime victimization (CBS, 2019; Notté et al., 2019).

When asked about the extent to which the nature and scope of these cyber threats have changed due to the COVID-19 outbreak, respondents either indicated that they could not yet assess this or stated that they did not see any immediate new threats. According to respondents, the types of cyber incidents have not changed, but this does not mean that there had been no changes during the pandemic. The most significant change reported by almost all respondents is that cybercriminals adapted their modus operandi to take advantage of the COVID-19 crisis. Additionally, some respondents mentioned an increase or expected increase in certain forms of online fraud.

"For example, the word 'Corona' or 'COVID-19' was often mentioned in the name of malicious apps, file names of malicious files, phishing domain links, or subject lines of phishing emails." (R2)

"We have observed phishing and banking malware that used corona as a theme. However, we did not see an increase in absolute numbers. Existing groups have adapted their scripts." (R4)

"Not directly new threats. However, corona was often part of the crime script. Furthermore, there were more reports of malicious webshops due to widespread online shopping." (R5)

"A change is that 'corona' was added as part of the pretext, as well as products that were highly sought after in this situation... fake webshops targeting fitness equipment and beauty products [gyms and beauty specialists/hairdressers closed]." (R7)

Respondents suspected that the increases in internet usage and remote work during the pandemic played a significant role in the rise of certain forms of cybercrime, such as the forms of online fraud mentioned above. One respondent reported that there is a:

"changing attack surface of organizations: increased remote work and accelerated digitalization of business processes have increased

[3] The questionnaire and SPSS syntax used for the analyses in this paper can be found in the following Open Science Framework repository: https://osf.io/6wefj/

attack opportunities, such as vulnerabilities discovered in Webex Meetings that could result in so-called 'ghost participants'. In addition, organizations have enabled remote logins by relaxing security measures." (R2)

"The number of internet users increased, and remote work increased as well. People are more dependent on the internet and using applications, including on their mobile devices." (R9)

Another respondent stated that:

"(...) it is plausible to see a relationship between the lockdowns and the increase in online shopping, even among people who did not or did so less frequently before and therefore had less experience. Additionally, people were forced to primarily communicate via phone and social media, again by individuals who did not or did so less frequently before and therefore had less experience." (R7)

However, respondents also mentioned another possible effect of increased remote work: people have more time to report incidents.

"Furthermore, it may also play a role that people were more often at home, making it easier for them to report incidents." (R5)

Finally, we asked the respondents about the impact of cybercrime during the pandemic. Most respondents indicated that this was not yet clear to them, but they generally believed that due to increased digital dependency, incidents with significant consequences for businesses are likely to occur more frequently.

"The more companies work digitally, the greater the opportunities for criminals and therefore the greater the impact. Companies have become more dependent on digital systems, making them more vulnerable if these fall into the hands of criminals." (R8)

"The impact of non-functioning systems due to DDoS attacks or the exploitation of vulnerabilities in online meeting platforms or VPN solutions has led to more consequences because more people have become dependent on them to continue their work." (R2)

One respondent also noted that attacks on the healthcare sector can cause significant disruptions.

"The impact of cyber incidents during the pandemic has increased in some cases. Particularly, ransomware with a disruptive effect on healthcare-related or logistical processes could cause more physical damage since in some cases, lives were at stake." (R2)

Overall, the exploratory interviews indicate that experts do not expect new cyber threats during the pandemic. However, they believe that the increase in remote work provides criminals with more opportunities to carry out their attacks, and they anticipate an increase in fraud-related offenses. Furthermore, experts report that due to increased reliance on digital systems, incidents can have a greater impact on organizations. Additionally, the COVID-19 pandemic has become a new and significant element in the modus operandi of cybercriminals, enabling them to better execute their attacks.

3.2. Quantitative survey

3.2.1. Comparison of the prevalence of cybercrime in 2019 and 2021

First, we examined the extent to which the prevalence of cybercrime increased or decreased during the COVID-19 pandemic. Table 1 shows what share of the citizens and SME-owners became a victim of cybercrime in the 12 months preceding the surveys in 2019 and 2021. The left part of the table shows the results for the total samples, including all respondents who participated in one or both of the surveys. The right part of the table shows the results with only the respondents who participated in both 2019 and 2021 surveys and were either citizens or SME owners in both years. By conducting this analysis with the exact same individuals being surveyed twice, we can exclude the possibility that changes in victimization of cybercrime are due to differences between samples. We will discuss the results of the total sample first and of those participating in both years next.

Table 1 shows that 28.6 % of the citizens reported being a victim of cybercrime in the past year in 2019, which increased to 32.3 % in 2021. Among SME owners, this increase was less pronounced: 31 % of them reported victimization in 2019, which slightly rose to 32.2 % in 2021. However, for both citizens and SME owners, this observed increase is not statistically significant. Therefore, no significant change has been observed in the prevalence of overall cybercrime victimization during the COVID-19 pandemic.

Although the overall prevalence of cybercrime does not appear to have changed, it is possible that victimization of certain types of cybercrime have increased during the pandemic. Therefore, the same comparisons were also made for each of the 10 types of cybercrime separately and for all cyber-enabled and cyber-dependent crimes combined. Table 1 shows that, among citizens, victimization of three types of cybercrime were reported more often in 2021 compared to 2019. Victimization due to phishing increased from 17.4 % to 20.8 %; victimization of consumer fraud increased from 5.6 % to 8.4 %; and the prevalence of DDoS-attacks increased from 0.5 % to 1.0 %. However, the results of the chi-square tests indicate that only the increase in consumer fraud is significant ($p < .05$). Furthermore, five types of cybercrime were reported less frequently by citizens in 2021 than in 2019: malware, ransomware, hacking, identity fraud, and online threats. Only the decrease in online threats from 3.6 % in 2019 to 1.8 % in 2021 is significant ($p < .05$). Additionally, the prevalence of cyberstalking (1 %) and online dating fraud (0.8 %) among citizens remained unchanged between 2019 and 2021.

Among SME owners, there is an increase in victimization for four

Table 1
Prevalence of cybercrime victimization among citizens and SME owners in 2019 and 2021.

	Total sample				Respondents participating in both waves			
	Citizens		SME owners		Citizens		SME owners	
	2019	2021	2019	2021	2019	2021	2019	2021
Any cybercrime	28.6 %	32.3 %	31.0 %	32.2 %	26.9 %	29.6 %	31.1 %	32.8 %
Any cyber-dependent crime	13.7 %	11.3 %	**15.3 %**	**11.2 %***	12.5 %	10.8 %	**16.6 %**	**10.0 %***
Malware	9.4 %	8.0 %	**10.4 %**	**6.9 %***	8.7 %	7.9 %	11.2 %	6.2 %
Ransomware	3.5 %	2.3 %	5.5 %	3.2 %	3.1 %	2.4 %	**7.9 %**	**2.9 %***
Hacking	3.6 %	2.1 %	4.7 %	3.4 %	2.9 %	1.9 %	**5.8 %**	**2.1 %***
DDoS attacks	0.5 %	1.0 %	1.1 %	0.7 %	0.2 %	1.2 %	0.8 %	0.8 %
Any cyber-enabled crime	23.2 %	27.5 %	25.3 %	28.3 %	21.4 %	25.5 %	25.3 %	28.6 %
Phishing	17.4 %	20.8 %	16.8 %	20.4 %	15.6 %	19.2 %	18.3 %	22.4 %
Cyberstalking	1.0 %	1.0 %	2.1 %	1.5 %	0.7 %	0.2 %	2.1 %	1.2 %
Identity theft	1.2 %	1.0 %	1.1 %	1.8 %	1.0 %	0.5 %	1.2 %	2.1 %
Consumer fraud	**5.6 %**	**8.4 %***	**4.7 %**	**7.8 %***	4.8 %	7.0 %	4.1 %	6.2 %
Online dating fraud	0.8 %	0.8 %	0.9 %	1.2 %	0.5 %	0.5 %	1.7 %	1.7 %
Online threats	**3.6 %**	**1.8 %***	6.8 %	5.0 %	**3.6 %**	**1.4 %***	6.2 %	4.6 %
N	604	799	529	678	416	416	241	241

Note: Differences between 2019 and 2021 tested with Chi-square tests: * $p < .05$; ** $p < .01$; *** $p < .001$.

forms of cybercrime. Victimization of phishing increased from 16.8 % in 2019 to 20.4 % in 2021, the prevalence of identity fraud increased from 1.1 % to 1.8 %, victimization of consumer fraud increased from 4.7 % to 7.8 %, and 1.2 % of the SME owners became a victim of online dating fraud in 2021 compared to 0.9 % in 2019. Only the increase in consumer fraud was significant ($p < .05$). The other six forms of cybercrime were reported less frequently by SME owners in 2019 than in 2021. The chi-square tests indicate that only the decrease in the prevalence of malware, from 10.4 % in 2019 to 6.9 % in 2021, is significant ($p < .05$).

Overall, victimization of cyber-dependent crime decreased among both citizens and SME owners, while victimization of cyber-enabled crime increased among both groups. However, only the decrease in victimization of cyber-dependent crime among SME owners was statistically significant ($p < .05$).

As described above, the right part of Table 1 shows the results when only respondents who participated in both waves were included. Overall, the patterns that were found were similar to those of the total sample, although the significance levels changed in some cases. Among citizens, the increase in consumer fraud was not significant anymore, while the decrease in online threats did remain statistically significant. Among the SME owners, both the decrease in malware and the increase in consumer fraud were not significant in this case. However, the decreases in the prevalence of ransomware and hacking became significant ($p < .05$).

3.2.2. *Cybercrime victimization during the COVID-19 pandemic*

The remaining analyses were conducted only among respondents who participated in the study in 2021 because these analyses focus on variables that were only measured in the second wave of the study. We present the results of these analyses for both SME owners and citizens together, as the number of respondents in a particular category (e.g., victims of a specific type of offense) was sometimes too small to warrant separate analyses between SMEs and citizens.

First, respondents who reported being victims of cybercrime in 2021 were asked whether, according to the victims themselves, the perpetrators exploited the COVID-19 crisis to commit the offense. Table 2 shows that particularly in the case of the three forms of online fraud, there was a relatively high incidence of COVID-19-related crime: approximately a quarter of the victims of consumer fraud (23.3 %), identity theft (25 %), and online dating fraud (28.6 %) reported that their victimization was COVID-19-related. This was also relatively often the case among victims of phishing (17.4 %) and ransomware (15 %). Only among victims of online threats (8.3 %) and DDoS-attacks (7.7 %), less than 10 % of the respondents report that their victimization was related to the pandemic. Overall, victims indicated in 15.9 percent of the cases that their cybercrime victimization was COVID-19 related and this percentage was higher among victims of cyber-enabled crime (18.3 %) than among cyber-dependent (11.8 %).

As shown in Table 3, we also examined whether victims who reported that their victimization was related to the pandemic perceived the offenses as more severe (measured on a scale of 1 'not very serious' to 3 'very serious'). Victims of all types of cybercrime, except identity theft, indicated that they perceived the offenses as more severe when they were COVID-19 related compared to when their victimization was unrelated to the pandemic, although these differences were only significant among victims of malware ($p < .001$), ransomware ($p < .05$), and phishing ($p < .01$). It is however important to note that for many types of cybercrime the number of victims was relatively low which could explain why no significant difference was found between the severity of COVID-19 related and unrelated offenses. When victims of all cyber-dependent crimes, all cyber-enabled crimes and all cybercrimes were combined, the COVID-19 related offenses were considered significantly more severe than the offenses that were unrelated to COVID-19 ($p < .001$).

Table 2
COVID-19 related victimization of cybercrime.

Type of crime	% COVID-19 related	Number of victims
Any cybercrime	**15.9 %**	**477**
Any cyber-dependent crime	**11.8 %**	**204**
Malware	11.7 %	111
Ransomware	15.0 %	40
Hacking	10.0 %	40
DDoS attacks	7.7 %	13
Any cyber-enabled crime	**18.3 %**	**524**
Phishing	17.4 %	304
Cyberstalking	11.1 %	18
Identity theft	25.0 %	20
Consumer fraud	23.3 %	120
Online dating fraud	28.6 %	14
Online threats	8.3 %	48

Table 3
Seriousness of cybercrime victimization.

	Unrelated to COVID-19		COVID-19 related	
Type of crime	Mean (s.d.)	n	Mean (s.d.)	n
Any cybercrime	**1.40 (0.61)**	**608**	**1.74 (0.73)*** **	**120**
Any cyber-dependent	**1.34 (0.56)**	**180**	**1.92 (0.65)*** **	**24**
Malware	**1.29 (0.54)**	**98**	**1.92 (0.76)*** **	**13**
Ransomware	**1.32 (0.59)**	**34**	**2.00 (0.63)***	**6**
Hacking	1.44 (0.61)	36	1.75 (0.50)	4
DDoS attacks	1.58 (0.52)	12	2.00 (n/a)	1
Any cyber-enabled	**1.43 (0.62)**	**428**	**1.70 (0.74)*** **	**96**
Phishing	**1.32 (0.55)**	**251**	**1.64 (0.76)** **	**53**
Cyberstalking	1.31 (0.60)	16	2.00 (1.41)	2
Identity theft	2.07 (0.70)	15	2.00 (1.00)	5
Consumer fraud	1.63 (0.69)	92	1.71 (0.66)	28
Online dating fraud	1.30 (0.68)	10	1.75 (0.96)	4
Online threats	1.48 (0.63)	44	1.75 (0.50)	4

Note: Differences between unrelated and related to COVID-19 tested with *t*-tests: * $p < .05$; ** $p < .01$; *** $p < .001$.

Respondents were also asked to indicate whether they suffered financial damage the last time they were victims of each type of cybercrime. Victims of malware, online threats, and DDoS-attacks reported no financial damage. Additionally, only one victim of hacking (€50), cyberstalking (€300), identity theft (€215), and online dating fraud (€500) reported financial damage and only two victims of ransomware (€30 and €1800) reported financial damage. Only among victims of phishing and consumer fraud there were more victims who experienced financial damage in 2021. Eight victims of phishing reported financial damage ranging from €40 to €2400 ($M = 603$; $SD = 798$). These amounts did not differ significantly between phishing offenses where the COVID-19 pandemic was exploited and those where it was not. Lastly, 76 victims of consumer fraud reported financial damage ranging from €5 to €5000 ($M = 283$; $SD = 743$). These amounts did not differ significantly either between offenses where the COVID-19 pandemic was exploited and those where it was not.

Next, we examined the associations between changes in internet usage and cybercrime victimization. Table 4 shows these results separately for internet usage at work, work-related internet usage at home, and private internet usage. The prevalence of cybercrime was highest among the group of respondents whose work-related internet usage at the workplace had strongly increased during the pandemic (41.3 %). Interestingly, victimization also occurred frequently among the group whose work-related internet usage at the workplace had strongly decreased (39.7 %). One possible explanation for this could be that they started using the internet more for work at home, where internet security may be less well regulated. The next row in Table 4 indeed shows that individuals whose work-related internet usage at home had strongly increased were also the most frequent victims (37.1 %), while those whose usage had strongly decreased were the least frequent victims (27.8 %). However, it is important to interpret these percentages carefully, as the number of respondents reporting a strong decrease ($n = 18$) or a slight decrease ($n = 25$) is relatively small. Moreover, both the

Table 4
Cyberccrime victimization by change in internet behavior at work and at home.

	Change in internet behavior…					
	Strongly decreased	Slightly decreased	Remained the same	Slightly increased	Strongly increased	N
At work	39.7 %	30.0 %	28.6 %	31.9 %	41.3 %	651
At home (work-related)	27.8 %	36.0 %	28.6 %	32.3 %	37.1 %	806
Private	**6.7 %**	**38.9 %**	**29.9 %**	**35.9 %**	**35.2 %***	**1477**

Note: Differences within each row were tested with Chi-square tests: * $p < .05$; ** $p < .01$; *** $p < .001$.

relationships between cybercrime victimization and work-related internet usage at work and at home were not statistically significant. Finally, Table 4 presents the prevalence of cybercrime victimization, divided by changes in private internet usage. Among the small group of 15 respondents whose internet usage strongly decreased during the COVID-19 crisis, the likelihood of victimization is significantly lower (6.7 %). Interestingly, the majority of victims, however, are found in the group whose internet usage only slightly decreased (38.9 %), although the differences with the groups reporting a slight increase (35.9 %) or a strong increase (35.2 %) in private internet usage are small. These differences are statistically significant ($p < 0.05$).

Finally, respondents were asked whether they had to use new applications or programs for their work or activities since the outbreak of the coronavirus. Table 5 shows the relationship between the use of new applications and programs and cybercrime victimization. Respondents who use new applications or programs at work are significantly more likely ($p < .05$) to become victims of cybercrime (36.3 %) compared to those who do not (28.8 %). Similarly, respondents who had to use new applications or programs for their work at home (36.1 %) are more likely to be victims compared to those who did not (30.9 %), although this difference is not statistically significant. The analyses from Table 5 were also conducted separately for civilians and SME owners. These additional analyses reveal a similar pattern for both groups, but none of the results are statistically significant. This may be due to reduced statistical power after splitting the sample.

4. Discussion

In this study we examined the impact of the COVID-19 pandemic on the prevalence, nature, and consequences of cybercrime among Dutch citizens and SMEs. In addition to conducting 10 qualitative interviews with experts in the field of cybersecurity to gain insight from the field, a panel of citizens and SME owners who were surveyed in 2019 and/or 2021 was used to gather self-reported data on cybercrime victimization.

The results of this research indicate that there was only a small, non-statistically significant increase in the prevalence of cybercrime during the pandemic compared to two years earlier, both among citizens and SME owners. Although the prevalence of cybercrime victimization among citizens only increased with 2.7–3.7 percent, this would still suggest that the number of cybercrime victims in the Netherlands increased with approximately half a million persons. This increase is, however, considerably lower than the 64 percent increase in police registrations for cybercrime in the Netherlands that was found by Kruisbergen and colleagues (2021). Moreover, since the increased prevalence found in this study was not statistically significant, it should be interpreted with caution.

A possible reason that no significant increase in cybercrime victimization was found in the current study may be the limited statistical power. Although over a thousand respondents participated in one or both waves of the study, the number of respondents might have been too low to detect small effect sizes, especially after splitting the sample into citizens and SME owners and after excluding respondents who only participated in one wave. It is also possible that the sudden shift from many offline activities and work to the online environment made people more aware of the risks of online behavior and, as a result, they have been more cautious in their online behavior. In this regard, a study found that in the aftermath of COVID-19 more people adopted online self-protection measures in their computer such as antivirus software and/or firewalls (Hawdon et al., 2020), which may have reduced victimization by cyber-dependent crimes. Moreover, it could be the case that online risks were already omnipresent prior to the outbreak of the COVID-19 pandemic. In this scenario there may have been a ceiling effect and the pandemic and the accompanying shift to more online activities could hardly further increase the online risks that people were already exposed to.

Table 5
Cybercrime victimization by use of new applications/programs at home or work.

	No new applications/programs	New applications/programs	N
At work	**28.8 %**	**36.3 %***	**680**
At home	30.9 %	36.1 %	810

Note: Differences within each row were tested with Chi-square tests: * $p < .05$; ** $p < .01$; *** $p < .001$.

Also when examining the ten types of cybercrime included in this study separately (i.e., malware, ransomware, phishing, hacking, cyberstalking, identity fraud, consumer fraud, online dating fraud, online threats, and DDoS-attacks), most offenses did not show any significant changes in prevalence. Only online threats among citizens and malware infections among SME owners significantly decreased. On the other hand, consumer fraud victimization significantly increased among both citizens and SME owners. This finding is consistent with research conducted in the United Kingdom, which also found an increase in the prevalence of online consumer fraud based on official registrations (Buil-Gil et al., 2021a; Johnson and Nikolovska, 2022; Kemp et al., 2021). However, it is important to note that the increases in victimization of consumer fraud in our study were no longer statistically significant when only respondents who participated in both waves were considered. This suggests that the increase may be partially due to a different composition of the sample in 2021 compared to 2019. But it is also possible that these increased rates of consumer fraud were not significant anymore in the latter analyses due to the decreased statistical power as a consequence of the considerably lower sample sizes.

Our finding that overall cybercrime victimization did not significantly increase during the pandemic, and that some forms of cybercrime even decreased, contradicts most previous research on this topic. Virtually all studies based on official registrations found an increase in cybercrime victimization during the pandemic (Buil-Gil et al., 2021a, 2021b; Buil-Gil and Zeng, 2022; Johnson and Nikolovska, 2022; Kemp et al., 2021; Kruisbergen et al., 2021). However, some studies based on self-reported data from victims (Hawdon et al., 2020) and offenders (Weulen Kranenbarg et al., 2022) did not show any changes in the prevalence of cybercrime, consistent with the findings of this research. This discrepancy between trends found in official registrations and these self-report studies suggests that there may not have been an actual increase in cybercrime during the pandemic, but rather an increase in reporting and registration of cybercrime (*reporting effect*). In one of the qualitative interviews, an expert also mentioned that they expected people to report cybercrime more frequently during the pandemic because they were spending more time at home. Additionally, in the Netherlands, it became possible to file online reports for friend-in-need fraud starting from April 2020, which may have made it easier for

victims to report such incidents to the police.

While the results of this study thus do not show a significant increase of cybercrime during the COVID-19 pandemic, the modus operandi of cybercriminals did appear to have changed. Various experts noted in the qualitative interviews that some cybercriminals adapted their modus operandi during the pandemic to include aspects of the COVID-19 crisis. The quantitative analyses also revealed that a considerable proportion of the victims of all types of cybercrime (7.7 %−28.6 %) reported that the perpetrators exploited the pandemic when committing their offenses. This was particularly true for the various forms of fraud (identity theft, consumer fraud, online dating fraud), with approximately a quarter of the victims indicating such exploitation (23.3 %−28.6 %). This result demonstrates that the cybercriminal landscape is constantly evolving, with cybercriminals capitalizing on current events to develop new opportunities to victimize individuals. Naidoo (2020) draws a similar conclusion following a content analysis of documents related to 185 online fraud cases. Therefore, it is crucial to remain vigilant in combating cybercrime, continuously monitoring changes in the modus operandi of cybercriminals, and considering the fact that they exploit current societal issues.

Although a significant proportion of respondents reported being victims of cybercrime, the financial damage in most cases was relatively minor. For most types of cybercrime (i.e., malware, online threats, DDoS attacks, hacking, cyberstalking, identity fraud, and online dating fraud), no or only one respondent reported suffering financial losses, ranging from 50 to 500 euros. It is however possible that victims underestimate the actual financial losses of cybercrime if they do not take into account indirect costs, which may even be greater (Anderson et al., 2019). However, in the case of consumer fraud, there were many respondents who experienced financial losses, sometimes amounting to thousands of euros. From this perspective, it is problematic that this specific type of offense increased during the pandemic, potentially leading to an overall increase in the total financial damage caused by cybercrime.

Several interviewed experts also expressed concerns that the widespread shift to remote work increased the opportunities for cybercriminals, for example, due to the sudden frequent use of new applications for video calling and online meetings. The quantitative analyses also revealed that respondents who had to use new applications and programs for their work during the pandemic were significantly more likely to become victims of cybercrime. This underscores the importance for employers to be aware of the risks associated with the use of new applications and programs and to provide instructions to their employees on how to use them securely (Georgiadou et al., 2022).

Finally, although this study made a distinction between citizens and SME owners, the results between these two groups were very similar. For example, cybercrime victimization in 2021 was virtually the same for both groups. Previous research has also found similarities in results between citizens and SME owners (Van de Weijer et al., 2020). One possible explanation is that a significant portion of the SME owners in this study were self-employed individuals, and previous research has shown that the internet usage of almost all self-employed individuals in the Netherlands is a mix of personal and business activities (Veenstra et al., 2015). Therefore, it is difficult to differentiate between victimization as individuals and as businesses. Nevertheless, the finding that citizens and SME owners were victimized at similar rates suggests that cybercriminals did not specifically target SMEs during the COVID-19 pandemic.

4.1. Limitations

When interpreting the results of this study, it is important to consider several limitations. First, this study measures cybercrime victimization at only two points in time, in May 2019 and April/May 2021. Unlike various studies based on official records, which typically have monthly data over a long period (e.g., Buil-Gil et al., 2021a, 2021b; Kemp et al., 2021), it is not possible to examine whether there was a pre-existing increasing or decreasing trend in cybercrime victimization before the COVID-19 pandemic. For instance, if there were a long-term decrease in cybercrime victimization, the finding of this report that cybercrime did not significantly increase between 2019 and 2021 could actually indicate that the pandemic did lead to more cybercrime. However, data on self-reported victimization in the Safety Monitor by Statistics Netherlands (CBS, 2020) show no decrease in cybercrime in the Netherlands between 2012 and 2019; instead, there is evidence of an increasing trend since 2016.[4] This strengthens our conclusion that cybercrime victimization did not significantly increase due to the COVID-19 pandemic. Nevertheless, it is also important to note that the current study only measures whether or not respondents fell victim to cybercriminals and not how often they were victimized. If victims in 2021 experienced more cyber incidents than victims in 2019, there would be a larger increase in cybercrime than reflected in the results of this study.

Second, respondents in this study were asked about cybercrime victimization during the year preceding April/May 2021. Since the “intelligent lockdown” in the Netherlands occurred between March 16, 2020, and May 31, 2020, the beginning of this lockdown was not fully captured in the measurement of victimization. It is likely that the most significant changes in our lives, work, and internet behavior occurred in the first weeks of this lockdown, making people most vulnerable to cybercrime attacks during that period. Indeed, Kruisbergen et al. (2021) demonstrate that the increase in registered cybercrime was highest during this first lockdown. The absence of an increase in cybercrime in the results of this study may therefore (partly) be due to the fact that victimization was not measured during these first weeks of the pandemic. However, if the prevalence of cybercrime did indeed increase during these first weeks, then there was no enduring effect of the shift from offline activities and work to online activities and work on victimization. Another drawback of questioning victimization over an entire year is that it does not allow for differentiation between victimization during different periods, such as (the end of) the first "intelligent lockdown" (March 16 - May 31, 2020), the period of relaxation of restrictions (June 1 - September 13, 2020), the period of limited restrictions (September 14 - December 13, 2020), and the second "hard lockdown" (December 14, 2020 - March 14, 2021). Since the extent of offline and online activities and work may have varied significantly during these periods, the prevalence of cybercrime could also fluctuate. Unfortunately, we were not able to measure this in the current study.

Third, respondents may not always be aware that they have been victims of cybercrime. Particularly in cases of hacking or malware infections, victims may never realize they have been targeted. The prevalence of these types of cybercrime may, therefore, be higher than indicated in this study. However, this applies to both the 2019 and 2021 measurements and only impacts the conclusions regarding (the lack of) changes in victimization during the pandemic if respondents become more aware of their victimization over time. This could be possible if respondents started using antivirus software more frequently, for example, because their employers made it mandatory when they had to work from home during lockdowns, and they received notifications of cybercriminal attacks or attempts. Consistent with this reasoning, our results indeed show that respondents who started using new applications or programs were more likely to become victims of cybercrime. However, our results also indicate that the prevalence of both malware and hacking decreased in 2021 compared to 2019 (although this decrease was significant only for SME owners in some analyses), which suggests that these new applications and programs did not lead to earlier detection of these types of cybercrime.

[4] The most recent version of the Safety Monitor of Statistics Netherlands (CBS, 2022) measured self-reported victimization of cybercrime in 2021. Unfortunately, the research methods and questions changed considerably which made it impossible to make comparisons with previous years.

Finally, the cybercriminal landscape is constantly changing, and technological developments continuously create new opportunities for committing cybercrime. An example is WhatsApp fraud, a specific form of friend-in-need fraud that has become prevalent in the Netherlands in recent years (Van 't Hoff-de Goede and Leukfeldt, 2021). To ensure optimal comparability between 2019 and 2021, we chose to keep the questionnaire and the different types of cybercrime queried exactly the same in this study. A disadvantage of this decision is that we may not capture newer forms of cybercrime, such as WhatsApp fraud, and therefore do not include them in the overall prevalence of cybercrime.

5. Conclusion

This study shows that cybercrime victimization among Dutch citizens and SMEs did not significantly increase during the COVID-19 crisis. The fact that official records of cybercrime did sharply increase (see, for example, Kruisbergen et al., 2021) suggests that victims were more likely to report their victimization. Although no significant increase in cybercrime victimization was found, the COVID-19 pandemic did have an impact on the modus operandi of cybercriminals: victims indicated that a considerable proportion of the offenses was related to the COVID-19 pandemic, particularly in the case of online fraud. Thus, cybercriminals seem to adapt their modus operandi to current societal developments. Finally, our results indicate that the use of new applications and programs for work was associated with an increased risk of cybercrime victimization during the COVID-19 crisis.

These conclusions have some important practical implications for the prevention of cybercrime victimization. First, it is of key importance that cyber security professionals raise awareness of how current societal developments – such as the COVID-19 pandemic – are exploited by cybercriminals for profit (e.g., COVID-19 themed malicious apps and phishing emails). Second, when employees have to use new computer programs for their work, it is important that they are trained on clear guidelines to use them safely and be aware of the potential risk involved. Third, the similarities in the results between citizens and SME owners suggest that both face and are similarly affected by cybercrime threats. This is consistent with the fact that Dutch SMEs have limited resources for cyber security (Moneva and Leukfeldt, 2023; Notte et al., 2019; Veenstra et al., 2015), which may not make a significant difference with private citizens. In such a case, SME owners could benefit from the same basic cyber security advice as individual users, albeit with minor adaptations to reflect the particular financial and organizational situation of SMEs.

CRediT authorship contribution statement

Steve van de Weijer: Conceptualization, Methodology, Formal analysis, Investigation, Writing – original draft, Funding acquisition. **Rutger Leukfeldt:** Conceptualization, Methodology, Investigation, Writing – review & editing, Funding acquisition. **Asier Moneva:** Writing – review & editing.

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Steve van de Weijer reports financial support was provided by Netherlands Organization for Scientific Research (NWO).

Data availability

The data that has been used is confidential.

Acknowledgements

This work was supported by the Netherlands Organization for Scientific Research (NWO) under project number NWA.1418.20.021.

References

Anderson, R., Barton, C., Boehme, R., Clayton, R., Ganan, C., Grasso, T., Levi, M., Moore, T., Vasek, M., 2019. Measuring the Changing Cost of Cybercrime. https://doi.org/10.17863/CAM.41598.

Bada, M., Nurse, J.R.C., 2019. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Inf. Comput. Secur. 27 (3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., Díaz-Castaño, N., 2021a. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. Eur.Soc. 23 (sup1), S47–S59. https://doi.org/10.1080/14616696.2020.1804973.

Buil-Gil, D., Zeng, Y., 2022. Meeting you was a fake: investigating the increase in romance fraud during COVID-19. J. Financ. Crime 29 (2), 460–475. https://doi.org/10.1108/JFC-02-2021-0042.

Buil-Gil, D., Zeng, Y., Kemp, S., 2021b. Offline crime bounces back to pre-COVID levels, cyber stays high: interrupted time-series analysis in Northern Ireland. Crime Sci. 10, 1–16. https://doi.org/10.1186/s40163-021-00162-9.

CBS, 2019. Cybersecurity Monitor 2019. Den Haag/Heerlen: CBS.

CBS, 2020. Veiligheidsmonitor 2019. Den Haag; Centraal Bureau voor de Statistiek.

CBS, 2022. Veiligheidsmonitor 2021. Den Haag; Centraal Bureau voor de Statistiek.

Cohen, L.E., Felson, M., 1979. Social change and crime rate trends: a routine activity approach. Am. Sociol. Rev. 44 (4), 588. https://doi.org/10.2307/2094589.

Coomans, A., Kühling-Romero, D., van Deuren, S., van Dijk, M., van de Weijer, S., Blokland, A., Eichelsheim, V., 2022. Stay home, stay safe? The impact of the covid-19 restrictions on the prevalence, nature, and type of reporter of domestic violence in the Netherlands. J. Fam. Violence 1–17. https://doi.org/10.1007/s10896-022-00473-8.

Georgiadou, A., Mouzakitis, S., Askounis, D., 2022. Working from home during COVID-19 crisis: a cyber security culture assessment survey. Secur. J. 35 (2), 486–505. https://doi.org/10.1057/s41284-021-00286-2.

Hawdon, J., Parti, K., Dearden, T.E., 2020. Cybercrime in America amid COVID-19: the initial results from a natural experiment. Am. J. Crim. Just. 45 (4), 546–562. https://doi.org/10.1007/s12103-020-09534-4.

Jones, P., 2022. Nature of Fraud and Computer Misuse in England and Wales: Year Ending March 2022. Retrieved from. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022.

Johns, E., Ell, M., 2023. Cyber Security Breaches Survey 2023. Retrieved from. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023.

Johnson, S.D., Nikolovska, M., 2022. The effect of COVID-19 restrictions on routine activities and online crime. J. Quant. Criminol. https://doi.org/10.1007/s10940-022-09564-7.

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., Díaz-Castaño, N., 2021. Empty streets, busy internet: a time-series analysis of cybercrime and fraud trends during COVID-19. J. Contemp. Crim. Justice 37 (4), 480–501. https://doi.org/10.1177/10439862211027986.

Kruisbergen, E., Haas, M., van Es, L., Snijders, J., 2021. De pandemie als criminologisch experiment. Justitiele Verkenningen 47 (3).

Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X., 2021. Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput. Secur. 105, 102248 https://doi.org/10.1016/j.cose.2021.102248.

Miró-Llinares, F., Moneva, A., 2019. What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks "Did cybercrime cause the crime drop? Crime Sci. 8 (1), 12. https://doi.org/10.1186/s40163-019-0107-y.

Moneva, A., Leukfeldt, R., 2023. Insider threats among Dutch SMEs: nature and extent of incidents, and cyber security measures. J. Criminol. https://doi.org/10.1177/26338076231161842.

Naidoo, R., 2020. A multi-level influence model of COVID-19 themed cybercrime. Eur. J. Inf. Syst. 29 (3), 306–321. https://doi.org/10.1080/0960085X.2020.1771222.

Nivette, A.E., Zahnow, R., Aguilar, R., Ahven, A., Amram, S., Ariel, B., Burbano, M.J.A., Astolfi, R., Baier, D., Bark, H.M., Beijers, J.E.H., Bergman, M., Breetzke, G., Concha-Eastman, I.A., Curtis-Ham, S., Davenport, R., Díaz, C., Fleitas, D., Gerell, M., Eisner, M.P., 2021. A global analysis of the impact of COVID-19 stay-at-home restrictions on crime. Nat. Hum. Behav. 5 (7), 868–877. https://doi.org/10.1038/s41562-021-01139-z.

Notte, R., Slot, L., Van 't Hoff de Goede, S., Leukfeldt, R., 2019. Cybersecurity in Het MKB: Nulmeting. Haagse Hogeschool. Den Haag. https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/cybersecurity-in-het-mkb_nulmeting_notte_et_al_2019.pdf.

Payne, B.K., 2020. Criminals work from home during pandemics too: a public health approach to respond to fraud and crimes against those 50 and above. Am. J. Crim. Justice 45 (4), 563–577. https://doi.org/10.1007/s12103-020-09532-6.

Ravindran, S., Shah, M., 2023. Unintended consequences of lockdowns, COVID-19 and the Shadow Pandemic in India. Nat. Hum. Behav. 7, 323–331. https://doi.org/10.1038/s41562-022-01513-5.

Staat van het MKB, 2021. Economisch Belang. Retrieved from. https://www.staatvanhetmkb.nl/themadashboard/economisch-belang.

Statistics Netherlands, 2018. Trends in Nederland 2018. Retrieved from. https://longreads.cbs.nl/trends18/maatschappij/cijfers/onderwijs/.
Statistics Netherlands, 2023. CBS Statline. Retrieved from. https://opendata.cbs.nl/statline/#/CBS/nl/dataset/37296ned/table?ts=1571893768002.
Stickle, B., Felson, M., 2020. Crime rates in a pandemic: the largest criminological experiment in history. Am. J. Crim. Just. 45 (4), 525–536. https://doi.org/10.1007/s12103-020-09546-0.
van de Weijer, S., Leukfeldt, R., van der Zee, S., 2020. Slachtoffer Van onlinecriminaliteit, Wat nu? Een onderzoek Naar Aangiftebereidheid Onder Burgers En Ondernemers. Politie en Wetenschap.
van 't Hoff-de Goede, S., Leukfeldt, R., 2021. WhatsAppfraude Komt Veelvuldig Voor in Nederland. CCV Secondant. Retrieved from. https://ccv-secondant.nl/platform/article/whatsappfraude-komt-veelvuldig-voor-in-nederland.
Veenstra, S., Zuurveen, R., Stol, W.Ph, 2015. Cybercrime Onder bedrijven. Een onderzoek Naar Slachtofferschap Van Cybercrime Onder Het Midden- en Kleinbedrijf En Zelfstandigen zonder Personeel in Nederland. Lectoraat Cybersafety, Leeuwarden. https://cybersciencecenter.nl/media/1054/2015-05-13-cybercrime-onder-bedrijven-def.pdf.
Weulen Kranenbarg, M., Weerman, F., 2022. Online jeugdcriminaliteit in coronatijd. Tijdschrift voor Criminol. 64 (4).

Steve van de Weijer is senior researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). His research interests include the life-course and criminal careers of offenders, intergenerational transmission of crime, biosocial influences on criminal behavior, victims and perpetrators of cybercrime, crime reporting behaviors and foreign national prisoners.

Rutger Leukfeldt is senior researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and holds the special chair of Governing Cybercrime at Leiden University. Furthermore, Rutger is the director of the Centre of Expertise Cybersecurity at The Hague University of Applied Sciences. His research focuses on the human factor in cybercrime.

Asier Moneva is a postdoc in the human factor of cybercrime at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and the Centre of Expertise Cyber Security of The Hague University of Applied Sciences. His interests include cybercrime, crime prevention, quantitative research methods, and open science.