nscr

Cybercriminaliteit tijdens de coronacrisis:

Aard, omvang en impact van cyberrisico's voor burgers en het mkb

Steve van de Weijer
Rutger Leukfeldt
Amsterdam, 2023

Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving

DE HAAGSE HOGESCHOOL

Cybercriminaliteit tijdens de coronacrisis:

Aard, omvang en impact van cyberrisico's voor burgers en het mkb

Steve van de Weijer[1] & Rutger Leukfeldt[1,2]

[1] Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)

[2] De Haagse Hogeschool, Centre of Expertise Cybersecurity

Acknowledgements: Dit onderzoek is uitgevoerd in het kader van *Kleine projecten NWA-routes 2020* als onderdeel van het project *Conflict resolution in an era of COVID-19* (dossiernummer NWA.1418.20.021), en werd gefinancierd door NWO.

1. Achtergrond

De uitbraak van het COVID-19 virus (i.e., coronavirus) in December 2019 in de Chinese stad Wuhan heeft een grote impact gehad op de manier van leven over de gehele wereld. Op 27 februari 2020 werd de eerste besmetting met het coronavirus in Nederland vastgesteld, waarna het aantal besmettingen snel opliep. Om de verdere verspreiding van het virus zo veel mogelijk te beperken werden er in Nederland – net als in de vrijwel alle andere landen – diverse vrijheid beperkende maatregelen ingesteld. Van 23 maart 2020 tot 1 mei 2020 gold in Nederland een zogenaamde 'intelligente lockdown' en werden mensen gevraagd om afstand van elkaar te houden, zo veel mogelijk thuis te blijven en werken, en werden scholen, sportclubs, horeca en winkels gesloten. In de twee jaar na de start van deze intelligente lockdown volgden er verschillende periodes met op- en afschalingen van restricties, waaronder nog twee 'harde lockdowns' die ingingen in december 2020 en december 2021.

Vanzelfsprekend hebben deze maatregelen een grote invloed gehad op onze manier van leven en werken en hebben er waarschijnlijk nog nooit zoveel Nederlanders tegelijk vanuit huis gewerkt als tijdens de coronacrisis. Dit heeft ook geleid tot veranderingen op het gebied van criminaliteit. In het eerste jaar van de coronapandemie lag het aantal geregistreerde misdrijven in Nederland ongeveer 6 procent lager dan in dezelfde periode in het jaar daarvoor, waarbij de verschillen het grootst waren tijdens de periodes met de strengste maatregelen (i.e., de intelligente lockdown en harde lockdown). Deze daling in geregistreerde criminaliteit was met name duidelijk terug te vinden onder misdrijven die doorgaans gepleegd worden als het slachtoffer niet in zijn of haar eigen huis is, zoals woninginbraak, zakkenrollenrij en fietsendiefstal (Kruisbergen et al., 2021). Voor huiselijk geweld, wat doorgaans binnen het eigen huis(houden) plaatsvindt, werd juist gevreesd voor een toename, maar deze lijkt achterwege te zijn gebleven in Nederland (Coomans et al., 2022).

Ook hebben verschillende experts in de media gewezen op de cyberrisico's van thuiswerken.[1] Dit is in het bijzonder voor midden- en kleinbedrijven (mkb) zeer relevant omdat mkb-bedrijven de ruggengraat vormen van de Nederlandse economie (zij zijn

[1] Zie bijvoorbeeld: https://www.bnr.nl/podcast/internet-vandaag/10404932/cybercriminelen-zien-kans-schoon-rond-thuiswerken
https://www.rtlnieuws.nl/nieuws/artikel/5057761/veilig-thuiswerken-vergaderen-vpn-corona
https://www.nrc.nl/nieuws/2020/03/23/bedrijven-zijn-niet-ingewerkt-op-dat-massale-thuiswerken-a3994642

verantwoordelijk voor 63% van het Bruto Binnenlands Product, 71% van de werkgelegenheid, en een totale omzet van 1023 miljard euro)[2], terwijl we ook weten dat deze groep bedrijven relatief vaak slachtoffer wordt van cyberaanvallen en weinig middelen ter beschikking heeft om zich hiertegen te wapenen (Leukfeldt, 2018). Tegelijkertijd zijn mkb-bedrijven waarschijnlijk niet goed ingericht op het ondersteunen van (massaal) thuiswerken en hebben daarom in allerijl en met veelal beperkte middelen moeten improviseren om het thuiswerken mogelijk te maken.

Dit onderzoek richt zich daarom op de vraag in hoeverre de uitbraak van het coronavirus en de daarmee gepaard gaande toename in thuiswerken gedurende de pandemie geleid hebben tot meer cyberonveiligheid voor zowel burgers als het mkb en wat we hiervan kunnen leren voor de toekomst. Hierbij kijken we naar de aard en omvang van dreigingen en incidenten en naar de impact die incidenten hebben gehad. Dit geeft inzicht in de wijze waarop plotselinge verschuivingen van offline naar online activiteiten leiden tot nieuwe cyberrisico's en is voor het mkb van groot belang om te kunnen beoordelen welke maatregelen zij kunnen en moeten nemen ten tijde van crises en wat die maatregelen mogen kosten. Uit eerder onderzoek weten we dat mkb-bedrijven weinig inzicht hebben in cyberrisico's (doordat aard en omvang vaak onduidelijk zijn) en daardoor niet weten welke maatregelen zij moeten treffen (Notte et al., 2019). Daarnaast hebben mkb-bedrijven vaak weinig middelen en kennis in huis om zich goed te kunnen wapenen tegen cybercriminelen. Drie onderzoeksvragen staan dan ook centraal in dit onderzoek:

1) *In hoeverre is de aard en omvang van cybercriminaliteit veranderd tijdens de coronapandemie?*
2) *Wat waren de gevolgen van slachtofferschap van cybercriminaliteit tijdens de coronapandemie?*
3) *Is er een relatie tussen veranderingen in internetgebruik en slachtofferschap van cybercriminaliteit tijdens de coronapandemie?*

Om deze vragen te beantwoorden analyseren we in fase 1 van dit onderzoek eerst de bestaande literatuur en interviewen we tien experts van de politie, cybersecuritybedrijven en andere relevante stakeholders. De literatuurstudie en verkennende interviews gebruiken we

[2] Zie: https://www.staatvanhetmkb.nl/themadashboard/economisch-belang

vervolgens in fase 2 van dit onderzoek om een vragenlijst te ontwikkelen die we hebben uitgezet onder een steekproef van burgers en een steekproef van mkb'ers om de aard, omvang en impact van slachtofferschap in kaart te brengen.[3] Hierdoor wordt een uniek beeld verkregen van de effecten van het coronavirus en veranderingen in ons internetgebruik.

[3] De auteurs danken dr. Jelle Groenendaal en dr. Asier Moneva voor hun bijdrage bij de uitvoering van een deel van het veldwerk van dit onderzoek.

2. Fase 1: Verkenning

2.1 Literatuurstudie

De vrijheid beperkende maatregelen die werden ingesteld om de verspreiding van het coronavirus te beperken, creëerden ook een perfect scenario om criminologische theorieën te toetsen en de pandemie werd zelfs al het grootste criminologische experiment in de geschiedenis genoemd (Stickle & Felson, 2020). Volgens de Routine Activiteiten Theorie (Cohen & Felson, 1979) worden mogelijkheden voor het plegen van criminaliteit gevormd door de herhaalde en veelvoorkomende routines van mensen. De vrijheid beprekende maatregelen gedurende de pandemie hadden een directe invloed op de dagelijks levens van mensen en beperkte de bewegingsvrijheid vaak tot het eigen huis. Als gevolg hiervan was er een verschuiving van offline naar online werk- en vrijetijdsactiviteiten (Buil-Gil et al., 2021), wat de mogelijkheden voor de meeste vormen van traditionele criminaliteit verminderden (e.g., Nivette et al., 2021), terwijl de mogelijkheden om cybercriminaliteit te plegen juist toenamen (Buil-Gil et al., 2021; Kemp et al., 2021; Miró-Llinares & Moneva, 2019).

De meeste empirische studies over de invloed van de coronacrisis op cybercriminaliteit maakten gebruik van *time-series analysis* waarin veranderingen in het aantal meldingen van diverse vormen van cybercriminaliteit, zoals online fraude, werden onderzocht. Diverse studies in het Verenigd Koninkrijk maakten bijvoorbeeld gebruik van de *Auction Fraud UK data* en vonden resultaten die in lijn waren met de Routine Activiteiten Theorie: meldingen van online fraude namen sterk toe tijdens de pandemie, met name tijdens de meest strenge lockdown periodes en de bijbehorende beperkte bewegingsvrijheid. (Buil-Gil et al., 2021; Buil-Gil & Zeng, 2022; Johnson & Nikolovska, 2022; Kemp et al., 2021). Deze toename was echter niet hetzelfde voor verschillende soorten cybercriminaliteit en fraude en voor verschillende slachtoffers. Zo bleek bijvoorbeeld dat online delicten zoals hacken en marktplaatsfraude toenamen, maar bijvoorbeeld fraude door babbeltrucs niet (Johnson & Nikolovska, 2022), en dat slachtofferschap van cybercriminaliteit met name toenam onder individuen maar niet onder bedrijven (Buil-Gil et al., 2021). Met betrekking tot datingfraude bleek bovendien dat de stijging in prevalentie tijdens de pandemie in het bijzonder groot was onder jonge slachtoffers en in mindere mate onder ouderen (Buil-Gil & Zeng, 2022). Ook een analyse van registraties van de Noord-Ierse politie bevestigt het algemene beeld van een

toename in cybercriminaliteit en fraude en benadrukt dat de pandemie de lange termijn trend van stijgende prevalentie van online criminaliteit heeft versneld (Buil-Gil et al., 2021).

Enkele internationale studies schetsen daarnaast een meer globaal beeld van de impact van de coronacrisis op cybercriminaliteit. Op basis van gegevens van de *World Health Organization* (WHO), in combinatie met nieuws artikelen, blog posts, online rapporten en social media berichten werd geconcludeerd dat grootschalige cyber aanvallen over de gehele wereld vaker voorkwamen na de uitbraak van het coronavirus (Lallie et al., 2021). Een thematische analyse van 185 documenten van *FraudWatch International* over verschillende gevallen van cyberfraude laat bovendien zien hoe cybercriminelen zich creatief aanpassen aan de fraudemogelijkheden die ontstaan door de dynamische context van de pandemie (Naidoo, 2020). Zo blijkt uit gegevens van de *US Federal Trade Commission* dat ouderen vaker slachtoffer werden, en meer economische schade ondervonden, van bepaalde vormen van fraude, zoals oplichting door criminelen die zich voordeden als medewerkers van technische ondersteuning of helpdesks (Payne, 2020). Wat betreft de cybersecurity cultuur, bleek uit een vragenlijst die in diverse Europese landen werd afgenomen onder 264 medewerkers in cruciale beroepen, dat 53 procent geen enkele begeleiding op het gebied van cybersecurity ontving gedurende de pandemie (Georgiadou et al., 2022), wat suggereert dat organisaties niet voorbereid waren op de cybersecurity uitdagingen die ontstonden tijdens de coronacrisis.

In lijn met het internationale onderzoek werd ook in Nederland een toename van geregistreerde cybercriminaliteit gevonden gedurende de pandemie. Kruisbergen et al. (2021) onderzochten veranderingen in politieregistraties van cybercriminaliteit, waar in hun onderzoek alle cybercriminaliteit in enge zin[4] onder valt en fraude met een online component (zoals Marktplaatsfraude en vriend-in-noodfraude). Zij toonden aan dat er in de eerste 52 weken van de pandemie 102.200 online misdrijven zijn geregistreerd door de politie, ten opzichte van 62.500 in dezelfde periode een jaar eerder. Dit is een stijging van 64%, welke overigens het sterkst was in de weken gedurende de eerste lockdown, toen er 112% meer

[4] Cybercriminaliteit in enge zin (i.e., *cyber-enabled crime*) omvat alle delicten waarbij ICT niet alleen het instrument is om het delict mee te plegen maar die ook gericht zijn op ICT, zoals hacken en malware. Cybercriminaliteit in brede zin (i.e., *cyber-dependent crime)* daarentegen omvat alle delicten waarbij ICT gebruikt wordt om het delict te plegen maar niet het doel is, zoals online bedreigingen of online fraude.

online delicten werden geregistreerd. Hierbij moet wel opgemerkt worden dat de stijgende trend in politieregistraties al was ingezet voorafgaand aan de eerste lockdown.

Over het algemeen laten deze internationale en Nederlandse studies dus een toename zien van de geregistreerde cybercriminaliteit tijdens de pandemie. Uit studies die gebruik maakten van zelfrapportages van slachtoffers en daders komt echter een ander beeld naar voren. Zo bleek uit een Amerikaanse studie waarin twee steekproeven dezelfde vragenlijst beantwoordden - één voor en één ten tijde van de pandemie – dat de online activiteiten en slachtofferschap van cybercriminaliteit van respondenten niet zijn veranderd tijdens de pandemie (Hawdon et al., 2020). In Nederland onderzochten Weulen Kranenbarg en Weerman (In druk) veranderingen in online activiteiten en het plegen van cybercriminaliteit met behulp van een longitudinale dataset met zelfrapportages van 289 jongeren (leeftijd 13-25 jaar) in het ICT-onderwijs (middelbare school en mbo). De resultaten van deze studie laten, zoals verwacht, een toename zien van online activiteiten en contacten met vrienden tijdens de eerste maanden van de pandemie terwijl offline activiteiten en contacten juist afnamen. De mate waarin deze jongeren cybercriminaliteit pleegden bleef grotendeels gelijk. Het overgrote deel van de jongeren rapporteerden net voor de start van de pandemie (januari-februari 2020) een zelfde mate van cybercriminaliteit als tijdens de pandemie (juni 2020), terwijl het percentage jongeren dat een afname rapporteerde groter was dan het percentage jongeren die aangeven meer cybercriminaliteit te zijn gaan plegen. Dit resultaat werd gevonden voor vrijwel elke afzonderlijke vorm van cybercriminaliteit, en overigens ook voor alle bevraagde vormen van traditionele cybercriminaliteit.

De discrepantie tussen deze resultaten van studies op basis van zelfrapportage en studies op basis van geregistreerde meldingen kan mogelijk verklaard worden door een registratie effect: dader- en slachtofferschap van cybercriminaliteit is gelijk gebleven maar slachtoffers melden hun slachtofferschap tijdens de pandemie vaker bij de politie of andere instanties. In Nederland werd het bijvoorbeeld vanaf april 2020 mogelijk om online aangifte te doen van vriend-in-nood-fraude, wat het mogelijk makkelijker maakte voor slachtoffers om naar de politie te stappen.

De huidige studie is de eerste Nederlandse studie waarin de invloed van de coronapandemie op slachtofferschap van cybercriminaliteit wordt onderzocht middels een slachtofferenquête. In tegenstelling tot de studie onder Amerikaanse slachtoffers van

Hawdon en collega's (2020) wordt er bovendien gebruik gemaakt van een panel, waardoor dezelfde respondenten zowel voor als tijdens de coronapandemie zijn ondervraagd en eventuele verschillen niet toe te schrijven zijn aan verschillen tussen steekproeven.

2.2 Verkennende interviews

Bij de start van het onderzoek interviewden we tien experts die werkzaam zijn bij verschillende publieke en private organisaties die door hun werkzaamheden zicht hebben op slachtofferschap van cybercriminaliteit (NCSC, MKB Nederland, Digital Trust Centre, Kamer van Koophandel, Nationale Politie, de Fraudehelpdesk, twee cybersecurity bedrijven en een verzekeraar). Het doel van deze interviews was om een eerste beeld op te halen van in hoeverre de aard en omvang van cyberdreigingen door de coronacrisis zijn veranderd en wat de aard, omvang en impact van cyberincidenten zijn ten tijde van de pandemie.

Op de vraag wat de belangrijkste cyberdreigingen waren *voor* het uitbreken van het coronavirus, geven respondenten diverse vormen van cybercriminaliteit aan. Meeste genoemd zijn ransomware en diverse varianten van fraudes gericht op online bankieren (phishing, banking malware, bankhelpdeskfraude). Daarnaast noemen respondenten, afhankelijk van de kernactiviteiten van hun organisatie, een hele reeks aan andere cybercrimes, variërend van vriend-in-nood-fraude, BEC-fraude en spionage. Dit beeld komt overeen met eerdere studies naar slachtofferschap van cybercrime.

Gevraagd naar in hoeverre de aard en omvang van deze cyberdreigingen veranderd zijn door het uitbreken van het coronavirus, geven respondenten aan dat ze dat ofwel (nog) niet kunnen inschatten, ofwel dat ze niet direct nieuwe dreigingen zien. De aard van cyberincidenten is volgens respondenten dus niet veranderd, maar dat wil niet zeggen dat er geen veranderingen zijn ten tijde van de pandemie. De grootste verandering die vrijwel alle respondenten rapporteren is dat de coronacrisis onderdeel is geworden van de modus operandi (i.e., de werkwijze) van cybercriminelen. Daarnaast geven enkele respondenten aan dat ze een toename zien of verwachten van bepaalde vormen van online fraude.

"Het woord Corona of COVID-19 werd wel vaak genoemd in de naam van de malafide app, bestandsnaam van malafide bestand, link van een phishingdomein of mailonderwerp van een phishingmail bijvoorbeeld."

"We hebben phishing en banking malware gezien die corona als thema hebben gebruikt. Maar in absolute aantallen zien we geen toename. Dus bestaande groepen hebben hun script aangepast."

"Niet direct nieuwe dreigingen. Wel was corona vaak onderdeel van het crime script. Verder meer meldingen van malafide webshops als gevolg van massaal online shoppen."

"Een verandering is dat 'corona' als onderdeel van de smoes erbij kwam, evenals producten die in deze situatie erg gewild waren. (…) nep-webshops die inspeelden op situatie met fitnessapparatuur en schoonheidsproducten (sportscholen en schoonheidsspecialisten/kappers gesloten)."

Respondenten vermoeden dat – in de gevallen waarbij er waarschijnlijk sprake is van een toename, zoals in de hierboven genoemde vormen van online fraude – het tijdens de coronapandemie veranderende internetgebruik en thuiswerken daar een belangrijke rol in speelt. Zo meldt een van de respondenten dat er sprake is van een

"[v]eranderend aanvalsoppervlak van organisaties: door thuiswerken en de versnelde digitalisering van bedrijfsprocessen zijn aanvalsmogelijkheden toegenomen, bijvoorbeeld op applicaties voor videobellen en online vergaderen. Zo werden er bijvoorbeeld kwetsbaarheden bekend in Webex Meetings die konden zorgen voor zogenaamde 'spookparticipanten'. Daarnaast hebben organisaties inloggen op afstand mogelijk gemaakt door veiligheidsmaatregelen te versoepelen."

"Het aantal internetgebruikers nam toe en ook het thuiswerken nam toe. Mensen zijn meer afhankelijk van het internet en het gebruik van applicaties ook op hun mobiele apparaat."

Een andere respondent geeft aan dat:

> *" (…) het ligt voor de hand een relatie te zien tussen de lockdowns en het toenemen van online winkelen, ook door mensen die dat voor die tijd niet of minder vaak deden en dus minder ervaren waren. Daarnaast onderhielden mensen noodgedwongen vooral contact via telefoon en social media, opnieuw ook weer door mensen die dit voorheen niet of minder deden en daardoor minder ervaring hadden."*

Maar respondenten melden ook een ander mogelijk effect van de toename in thuis werken: mensen hebben meer tijd om incidenten te melden:

> *"Verder kan ook meespelen dat mensen meer thuis waren en daardoor makkelijker meldden."*

Ten slotte vroegen we de respondenten naar de impact van cybercriminaliteit tijdens de coronapandemie. De meeste respondenten gaven aan daar (nog) geen zicht op te hebben, maar wel werd over het algemeen aangenomen dat doordat bedrijven meer afhankelijk zijn van digitalisering er waarschijnlijk vaker incidenten gebeuren met grote gevolgen voor die bedrijven:

> *"Hoe meer bedrijven digitaal werken, des te groter zijn de mogelijkheden voor criminelen en dus des te groter is de impact. Bedrijven zijn meer afhankelijk geworden van digitale systemen en dus kwetsbaarder als zij in handen komen van criminelen."*

> *"[D]e impact van niet werkende systemen bijvoorbeeld door een DDoS of het misbruiken van kwetsbaarheden in onlinevergaderplatformen of VPN-oplossingen hebben tot meer consequenties geleid, omdat meer mensen er van afhankelijk zijn geworden om hun werk te kunnen blijven doen."*

Ten slotte geeft een respondent aan dat aanvallen op de zorgsector kunnen zorgen voor grote verstoringen:

> *"De impact van cyberincidenten tijdens corona is in sommige gevallen toegenomen. Vooral ransomware met een verstorende werking in zorg-gerelateerde of logistieke processen konden nu meer fysieke schade veroorzaken aangezien in sommige gevallen mensenlevens op het spel stonden."*

Alles overziend laten de verkennende interviews zien dat experts niet verwachten dat de aard van cybercriminaliteit is veranderd tijdens de pandemie, maar wel dat het massale thuiswerken ervoor zorgt dat criminelen meer mogelijkheden hebben om hun aanvallen uit te voeren en dat slachtofferschap van mate name fraude-gerelateerde delicten zullen toenemen. Verder rapporteren experts dat door de toegenomen afhankelijkheid van digitale systemen incidenten een grotere impact kunnen hebben op organisaties en dat corona verder vooral een nieuwe en belangrijk onderdeel is van de modus operandi van criminelen om hun aanvallen beter uit te kunnen voeren.

3. Fase 2: Verdieping

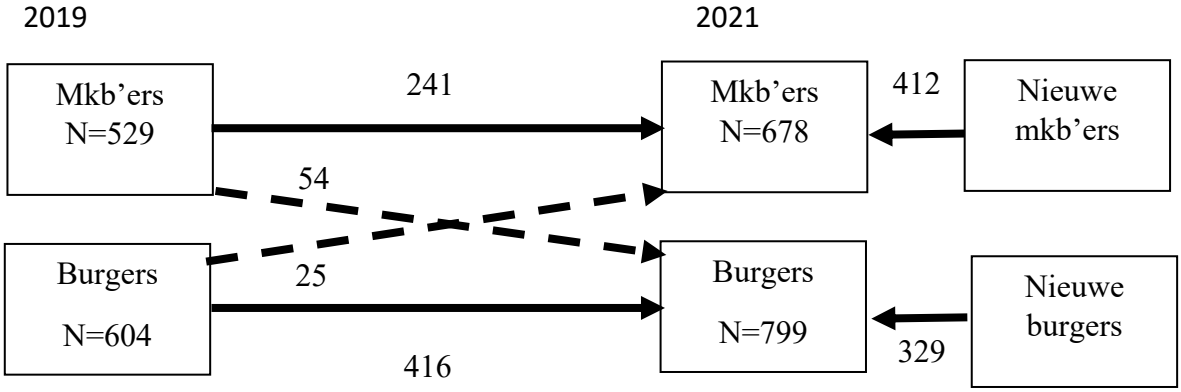
Om de inzichten uit de literatuur en verkennende interviews te toetsen en te verdiepen, zijn burgers en mkb'ers ondervraagd over hun ervaren slachtofferschap. We bespreken hierna eerst de methoden en daarna de resultaten van het vragenlijstonderzoek.

3.1 Methoden

3.1.1 Steekproef

Om veranderingen in slachtofferschap van cybercriminaliteit gedurende de coronapandemie te onderzoeken wordt in dit onderzoek gebruik gemaakt van gegevens die verzameld zijn door zowel in 2019 als in 2021 een vragenlijst uit te zetten onder deelnemers van het onderzoekspanel van I&O Research. De eerste ronde van de dataverzameling is gedaan tussen 2 en 13 mei 2019 in het kader van een onderzoek voor Politie en Wetenschap (Van de Weijer et al., 2020). Voor dit onderzoek hebben destijds 1133 respondenten vragen beantwoord over, onder andere, slachtofferschap van cybercriminaliteit. Deze respondenten zijn onderverdeeld in 529 mkb'er en 604 burgers. Respondenten in de eerste groep waren zzp'ers of zelfstandigen met personeel, terwijl de tweede groep bestaat uit mensen die in loondienst, studerend, werkeloos, of gepensioneerd waren.

Vervolgens hebben wij getracht om tussen 15 april en 17 mei 2021 – ruim een jaar na de start van de pandemie – dezelfde respondenten uit het onderzoekspanel van I&O Research te benaderen. Helaas bleek dat niet in alle gevallen mogelijk, omdat een aantal respondenten geen deel meer uitmaakte van het panel of niet deel kon of wilde nemen. In totaal zijn 241 mkb'ers uit de steekproef van 2019 opnieuw bevraagd in 2021, terwijl 416 burgers in beide jaren deelnamen. Daarnaast kwam het 25 keer voor dat een respondent in 2019 als burger deelnam, maar in 2021 inmiddels een mkb'er was geworden. De omgekeerde situatie – mkb'er in 2019 en burger in 2021 – kwam 54 keer voor. Om de steekproef verder op te vullen is besloten om de vragenlijst ook uit te zetten onder respondenten die in 2019 niet mee hebben gedaan. Dit heeft geleid tot 412 mkb'ers en 329 burgers die alleen in 2021 mee deden. De totale steekproeven in 2021 bestaan zodoende uit 678 mkb'ers en 799 burgers. De steekproef wordt in onderstaande figuur samengevat.



3.1.2 Variabelen

Slachtofferschap van cybercriminaliteit is gemeten door zowel in 2019 als 2021 aan de respondenten te vragen of ze ooit slachtoffer zijn geworden van tien soorten cybercriminaliteit (i.e., malware, ransomware, phishing, hacking, cyberstalking, identiteitsfraude, aan- en verkoopfraude, online dating fraude, online bedreigingen, DDoS aanvallen). Respondenten konden hierbij aangeven dat dit in de afgelopen 12 maanden is gebeurd, dat dit langer geleden is gebeurd, of dat dit niet is gebeurd. In dit onderzoek maken wij enkel onderscheid tussen respondenten die in de afgelopen 12 maanden slachtoffer werden en zij die dit niet werden in de afgelopen 12 maanden. Zodoende kunnen we een vergelijking maken tussen de prevalentie van cybercriminaliteit gedurende de pandemie (april/mei 2020 tot april/mei 2021) en voorafgaand aan de pandemie (mei 2018 tot mei 2019). Voor elk van de afzonderlijke typen cybercriminaliteit is een dichotome variabele aangemaakt die aangeeft of respondenten slachtoffer zijn geworden of niet. Daarnaast is er nog een overkoepelende variabele aangemaakt die aangeeft of respondenten van minimaal 1 soort delict slachtoffer is geweest of niet.

De angst om slachtoffer van cybercriminaliteit te worden is ook in zowel 2019 als 2021 gemeten, in beide jaren middels onderstaande 8 items. Respondenten konden hier op antwoorden met een 5-puntsschaal lopend van helemaal oneens tot helemaal eens.

- Ik ben bang om slachtoffer te worden van cybercriminaliteit in de nabije toekomst.
- Het idee dat iemand zonder toestemming in mijn online bankrekening kan inloggen, maakt me bang.

- Ik maak me zorgen dat ik slachtoffer kan worden van phishing.
- Ik maak me druk over de mogelijkheid dat mijn computer gehackt kan worden.
- Ik denk dat het makkelijk kan gebeuren dat ik online word opgelicht.
- Dat er ransomware op mijn computer kan komen, maakt me ongerust.
- Het is goed mogelijk dat ik het komende jaar slachtoffer word van cybercriminaliteit.
- Als ik slachtoffer zou worden van cybercriminaliteit, zou dat ernstige gevolgen kunnen hebben.

De Cronbach's alpha van deze schaal was .88 in 2019 en .90 in 2021 wat aangeeft dat de interne consistentie van deze schaal (zeer) goed is.

De overige variabelen die gebruikt zijn in deze studie zijn alleen gemeten in 2021, in de meeste gevallen omdat ze direct betrekking hebben op de coronapandemie. Zo is aan alle respondenten die in de laatste twaalf maanden slachtoffer werden van een specifiek type cybercriminaliteit bijvoorbeeld gevraagd of er door dader(s) misbruik is gemaakt van de coronacrisis. Ook werd aan deze slachtoffers gevraagd of ze, de laatste keer dat ze van een bepaald delict slachtoffer werden, financiële schade hebben geleden, en zo ja hoeveel. Daarnaast konden respondenten die de laatste twaalf maanden slachtoffer werden aangeven hoe ernstig ze dit delict zelf hebben ervaren. Hierbij konden respondenten kiezen uit drie antwoordmogelijkheden: niet zo ernstig (1), redelijk ernstig (2), bijzonder ernstig (3).

Daarnaast zijn respondenten gevraagd naar veranderingen in hun internetgebruik gedurende de coronapandemie, middels onderstaande drie vragen:

- In hoeverre is uw werk-gerelateerde internetgebruik op het werk (bijv. op kantoor, werkplaats, op locatie bij klanten) toe- of afgenomen sinds de uitbraak van het coronavirus?
- In hoeverre is uw werk-gerelateerde internetgebruik thuis toe- of afgenomen sinds de uitbraak van het coronavirus?
- In hoeverre is uw internetgebruik in privé-tijd toe- of afgenomen sinds de uitbraak van het coronavirus?

Op al deze drie vragen konden respondenten antwoorden op een 5-puntsschaal, variërend van sterk afgenomen (1) tot sterk toegenomen (5), of aangeven dat een vraag niet van toepassing is. Daarnaast zijn respondenten gevraagd of ze voor werk-gerelateerde

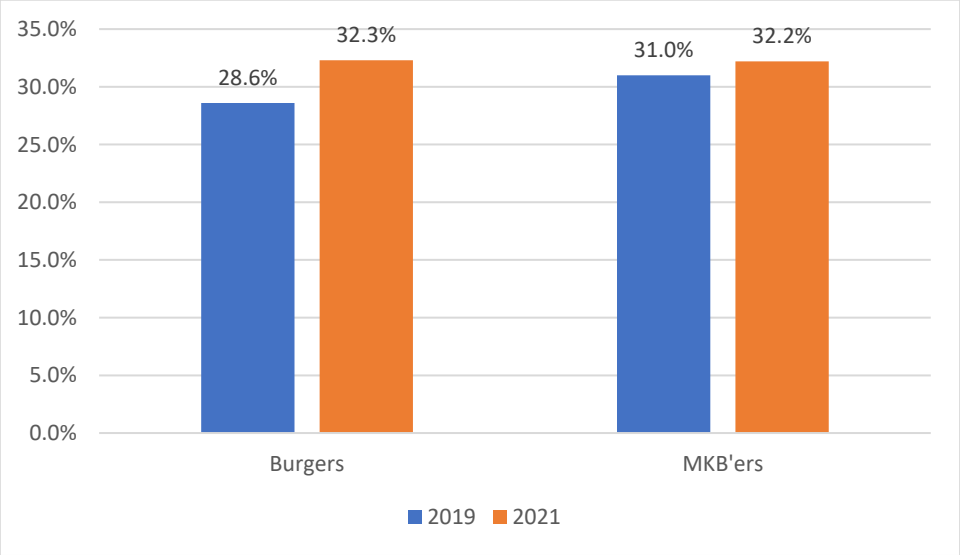
werkzaamheden, op het werk en thuis, nieuwe applicaties of programma's op de computer moeten gebruiken, sinds de uitbraak van het coronavirus.

3.2 Resultaten

3.2.1 Vergelijking van prevalentie van, en angst voor, cybercriminaliteit in 2019 en 2021

Ten eerste is onderzocht in welke mate de prevalentie van cybercriminaliteit is toe- of afgenomen ten tijden van de coronapandemie. Figuur 1 toont het aantal burgers en mkb'ers dat in 2019 en 2021 heeft aangegeven slachtoffer te zijn geworden van ten minste één soort cybercriminaliteit in de voorafgaande 12 maanden. In 2019 gaf 28.6% van de burgers aan het afgelopen jaar slachtoffer te zijn geweest van cybercriminaliteit, wat steeg naar 32.3% in 2021. Onder mkb'ers was deze stijging minder groot: 31% van hen rapporteerde slachtofferschap in 2019, wat licht steeg naar 32.2% in 2021. Voor zowel burgers als mkb'ers geldt echter dat de gevonden stijging niet significant is. Er is dus geen significante verandering waargenomen in de prevalentie van cybercriminaliteit ten tijden van de coronapandemie.

Figuur 1: Prevalentie cybercriminaliteit in 2019 en 2021

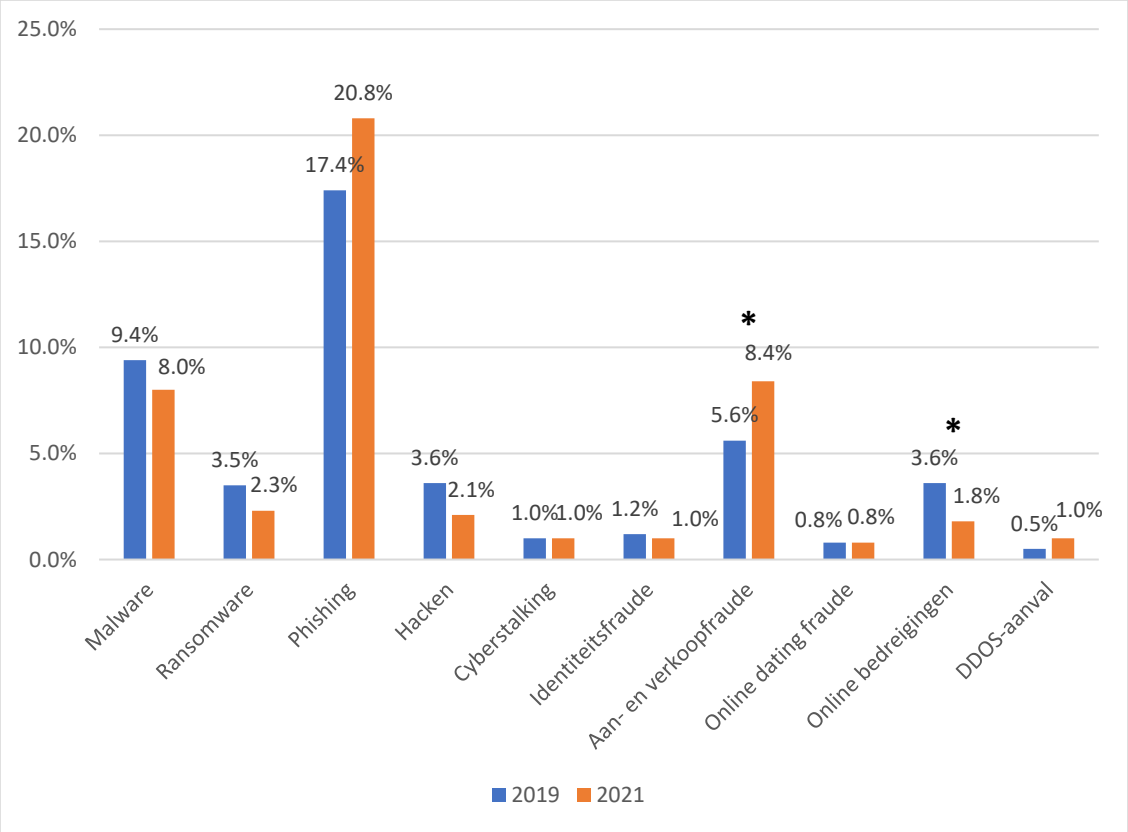


Alhoewel de prevalentie van cybercriminaliteit in zijn totaliteit dus niet lijkt te zijn veranderd, is het wel mogelijk dat bepaalde vormen van cybercriminaliteit zijn toegenomen tijdens de pandemie. Daarom is dezelfde vergelijking ook uitgevoerd voor alle 10 soorten cybercriminaliteit apart. Figuur 2 toont de resultaten van deze analyses onder de steekproef

van burgers. Hieruit blijkt dat er slechts drie soorten cybercriminaliteit zijn waarvan de respondenten rapporteren dat zij hier in 2021 vaker slachtoffer van werden dan in 2019. Slachtofferschap van phishing steeg van 17.4% naar 20.8%; slachtofferschap van aan- en verkoopfraude van 5.6% naar 8.4%; en de prevalentie van DDOS-aanvallen steeg van 0.5% naar 1.0%. De resultaten van de chi-kwadraattoetsen laten echter zien dat er alleen bij aan- en verkoopfraude sprake is van een significante stijging in slachtofferschap (p<.05).

Daarnaast blijkt uit Figuur 2 dat 5 soorten cybercriminaliteit minder vaak werden gerapporteerd in 2021 dan in 2019: malware, ransomware, hacken, identiteitsfraude, en online bedreigingen. Alleen de daling van online bedreigingen van 3.6% in 2019 naar 1.8% in 2021 is significant (p<.05). Daarnaast is de prevalentie van slachtofferschap van cyberstalking (1%) en online dating fraude (0.8%) gelijk gebleven tussen 2019 en 2021.

Figuur 2: Prevalentie 10 soorten cybercriminaliteit onder burgers, in 2019 en 2021

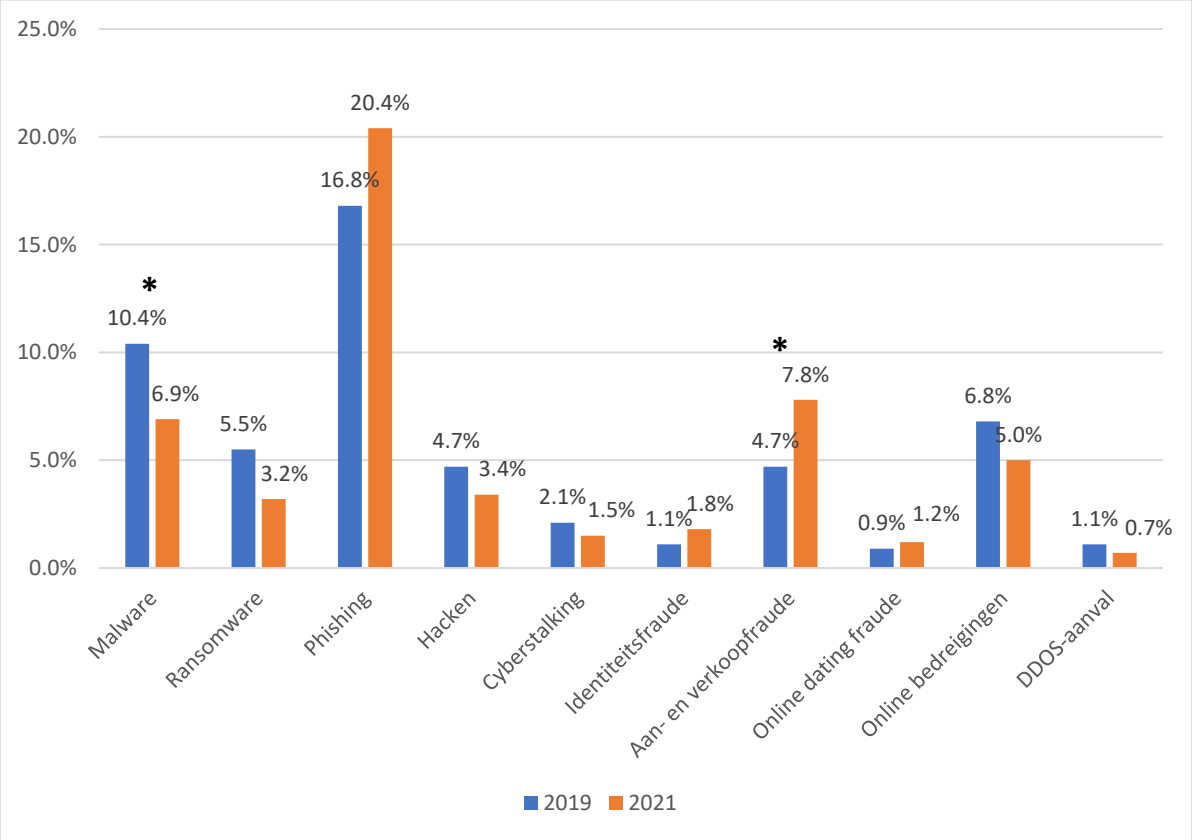


*Noot: *p<.05*

Figuur 3 laat vervolgens de vergelijking van de prevalentie van de verschillende soorten cybercriminaliteit onder mkb'ers zien. Onder de mkb'ers is er slechts sprake van een

stijging in slachtofferschap bij vier vormen van cybercriminaliteit. Slachtofferschap van phishing steeg van 16.8% in 2019 naar 20.4% in 2021, de prevalentie van identiteitsfraude steeg van 1.1% naar 1.8%, slachtofferschap van aan- en verkoopfraude steeg van 4.7% naar 7.8%, en 1.2% van de mkb'ers werd in 2021 slachtoffer van online dating fraude ten opzichte van 0.9% in 2019. Opnieuw is echter alleen de stijging in aan- en verkoopfraude significant ($p<.05$). De overige zes vormen van cybercriminaliteit werden juist minder vaak gerapporteerd door mkb'ers in 2019 dan in 2021. De chi-kwadraattoetsen laten echter zien dat alleen de daling in malware, van 10.4% in 2019 naar 6.9% in 2021, significant was ($p<.05$).

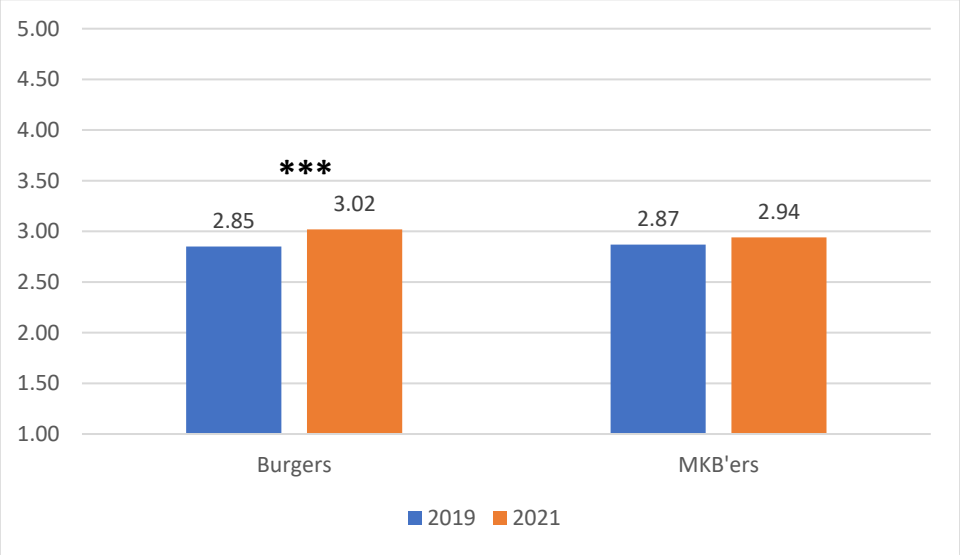
Figuur 3: Prevalentie 10 soorten cybercriminaliteit onder mkb'ers, in 2019 en 2021



*Noot: *p<.05*

Tot slot worden in Figuur 4 de gemiddelden scores op de schaal (lopend van 1 tot 5) voor angst voor cybercriminaliteit weergegeven. Onder burgers was er sprake van een significante stijging van deze gemiddelde score van 2.85 in 2019 naar 3.02 in 2021 ($p<.001$). Onder mkb'ers was deze stijging minder groot en niet significant, met gemiddelde scores van 2.87 in 2019 naar 2.94 in 2021.

Figuur 4: Angst voor cybercriminaliteit in 2019 en 2021



*Noot: ***p<.001*

De analyses uit Figuur 1 tot en met 4 zijn nog een keer herhaald met alleen de respondenten die zowel in 2019 als in 2021 hebben mee gedaan aan de enquête, en tevens in beide jaren burger of in beide jaren mkb'er waren. Doordat in deze analyse exact dezelfde mensen twee keer zijn ondervraagd, sluiten we uit dat veranderingen in slachtofferschap van, en angst voor, cybercriminaliteit het gevolg zijn van verschillen tussen de steekproeven. In de Appendix zijn de figuren weergegeven van deze additionele analyse. De resultaten komen in grote lijnen overeen met de hierboven omschreven resultaten. Het grootste verschil is dat zowel bij burgers als mkb'ers de stijging in de prevalentie van aan- en verkoopfraude niet meer significant is, wanneer alleen deze groep wordt meegenomen. Daarnaast is bij de groep mkb'ers die beide jaren deelnamen de daling in slachtofferschap van ransomware ($p<.05$) en hacking ($p<.05$) significant, en die van malware juist niet meer.

3.2.2 Slachtofferschap cybercriminaliteit gedurende de COVID-19 pandemie

Het restant van de analyses is alleen uitgevoerd onder de respondenten die in 2021 deelnamen aan de studie omdat deze analyses betrekking hebben op variabelen die alleen in de tweede wave van het onderzoek zijn gemeten. We presenteren de resultaten van deze analyses voor de mkb'ers en burgers samen, omdat het aantal respondenten in een bepaalde

categorie (bijv. slachtoffers van een specifiek type delict) soms te klein is om een opsplitsing te maken tussen mkb'ers en burgers.

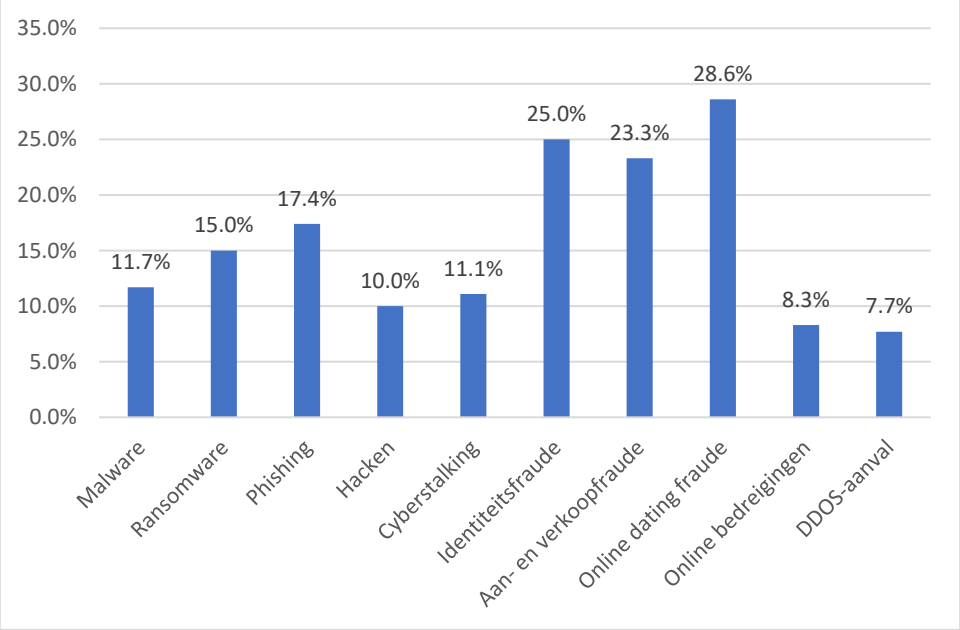
Allereerst is aan de respondenten, die rapporteerden dat ze slachtoffer zijn geweest van cybercriminaliteit, gevraagd of de daders van het delict, volgens de slachtoffers, misbruik maakten van de coronacrisis. Figuur 5 laat zien dat met name bij de drie vormen van online fraude er relatief vaak sprake was van corona-gerelateerde criminaliteit: ongeveer een kwart van de slachtoffers van aan-en verkoopfraude (23.3%), identiteitsfraude (25%), en online dating fraude (28.6%) rapporteerde dat hun slachtofferschap corona-gerelateerd was. Ook onder slachtoffers van phishing (17.4%) en ransomware (15%) werd dit relatief vaak gerapporteerd. Alleen onder slachtoffers van online bedreigingen (8.3%) en DDoS-aanvallen (7.7%) rapporteerden minder dan 10% van de respondenten dat de daders misbruik maakten van de pandemie.

In een additionele analyse (niet weergegeven in Figuur 5) is ook onderzocht of slachtoffers die aangeven dat de daders misbruik maakten van de pandemie, de delicten ook als ernstiger ervaarden (gemeten op een schaal van 1 'niet zo ernstig' tot 3 'bijzonder ernstig'). Onder slachtoffers van malware ($p<.001$), ransomware ($p<.05$), en phishing ($p<.001$) bleek het inderdaad zo te zijn dat de corona-gerelateerde delicten als ernstiger werden ervaren door de slachtoffers. Bij de andere delicten werd geen significant verschil gevonden in de ernst van het delict.

De respondenten zijn ook gevraagd om aan te geven of ze financiële schade hebben geleden de laatste keer dat ze slachtoffer werden van iedere vorm van cybercriminaliteit. De slachtoffers van malware, online bedreigingen, en DDoS-aanvallen rapporteerden geen van allen financiële schade. Daarnaast gaf slechts één van de slachtoffers van hacking (50€), cyberstalking (300€), identiteitsfraude (215€), en online datingfraude (500€) aan financiële schade te hebben, terwijl slechts 2 slachtoffers van ransomware (30€ en 1800€) financiële schade rapporteerden. Enkel onder slachtoffers van phishing en aan- en verkoopfraude waren er meer slachtoffers met financiële schade. Acht slachtoffers van phishing hadden financiële schade geleden, variërend van 40€ tot 2400€ (gemiddelde: 603€; s.d.: 798€). Deze bedragen verschilden niet significant tussen phishing delicten waarbij misbruik werd gemaakt van de coronapandemie en niet. Tot slot rapporteerden 76 slachtoffers van aan- en verkoopfraude financiële schade, variërend van 5€ tot 5000€ (gemiddelde: 283€; s.d.: 743€).

Ook deze bedragen verschilden niet significant tussen de delicten waarbij misbruik werd gemaakt van de coronapandemie en niet.

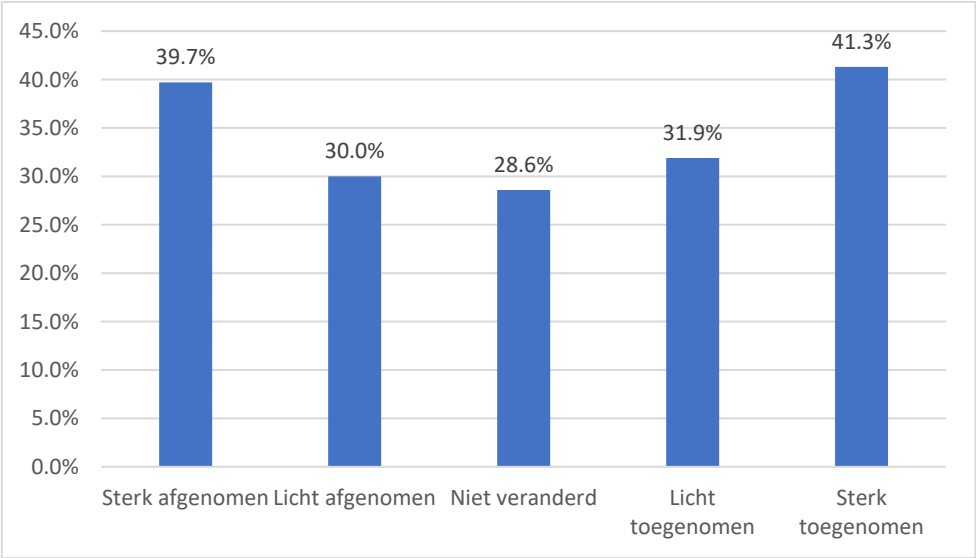
Figuur 5: Corona-gerelateerd slachtofferschap



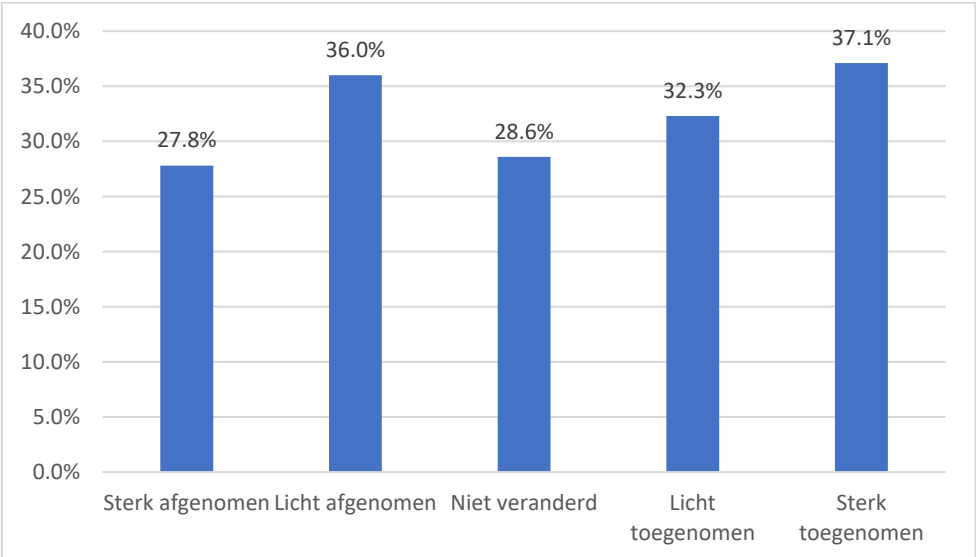
Vervolgens is onderzocht in hoeverre veranderingen in internetgebruik samenhangen met slachtofferschap. Figuur 6 toont het verband aan tussen slachtofferschap van cybercriminaliteit en veranderingen in werk-gerelateerd internetgebruik op het werk. Uit deze figuur blijkt dat de prevalentie van cybercrime het hoogst was onder de groep respondenten wiens werk-gerelateerd internetgebruik op het werk sterk is toegenomen tijdens de pandemie (41.3%). Opvallend genoeg kwam slachtofferschap ook vaak voor onder de groep wiens werk-gerelateerd internetgebruik op het werk juist sterk is afgenomen (39.7%). Een mogelijke verklaring hiervoor zou kunnen zijn dat zij juist thuis het internet meer zijn gaan gebruiken voor werk, waar de internetbeveiliging wellicht minder goed geregeld is. Figuur 7 laat het verband zien slachtofferschap van cybercriminaliteit en werk-gerelateerd internetgebruik thuis. Hieruit blijkt inderdaad dat de personen bij wie het werk-gerelateerd internetgebruik in eigen huis het sterkst is toegenomen ook het vaakst slachtoffer worden (37.1%), terwijl degene waarbij het sterk is afgenomen het minst vaak slachtoffer worden (27.8%). Desalniettemin blijkt ook de groep die een lichte afname in werk-gerelateerd internetgebruik thuis rapporteert relatief vaak slachtoffer te worden (36%). Enige

voorzichtigheid bij de interpretatie van deze percentages echter wel geboden, aangezien het aantal respondenten dat een sterke (n=18) of lichte afname (n=25) rapporteert relatief klein is. Bovendien zijn de relaties tussen slachtofferschap en internetgebruik, zoals weergegeven in Figuur 6 en 7 beide niet significant.

Figuur 6: Slachtofferschap cybercriminaliteit, opgesplitst naar verandering in internetgebruik op werk

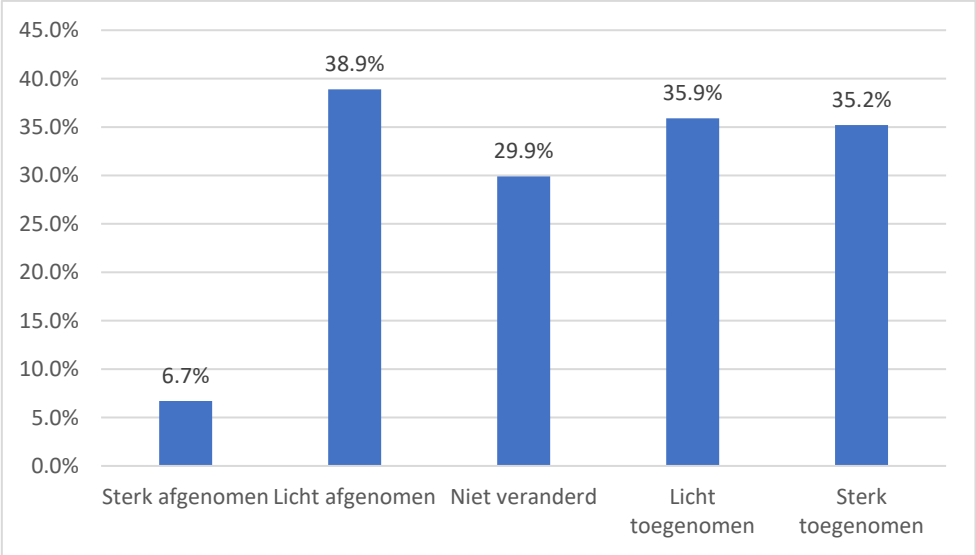


Figuur 7: Slachtofferschap cybercriminaliteit, opgesplitst naar verandering in werk-gerelateerd internetgebruik thuis



Figuur 8 geeft de prevalentie van slachtofferschap van cybercriminaliteit weer, opgesplitst naar de verandering in privé internetgebruik. Onder de kleine groep van 15 respondenten wiens internetgebruik sterk is afgenomen tijdens de coronacrisis is de kans op slachtofferschap veruit het kleinst (6.7%). Opvallend genoeg zijn de meeste slachtoffers echter te vinden in de groep wiens internetgebruik licht is afgenomen (38.9%), al zijn de verschillen klein met de groepen die een lichte (35.9%) of sterke (35.2%) toename in privé internetgebruik rapporteerden. De verschillen in slachtofferschap tussen de groepen in Figuur 8 zijn significant ($p<.05$).

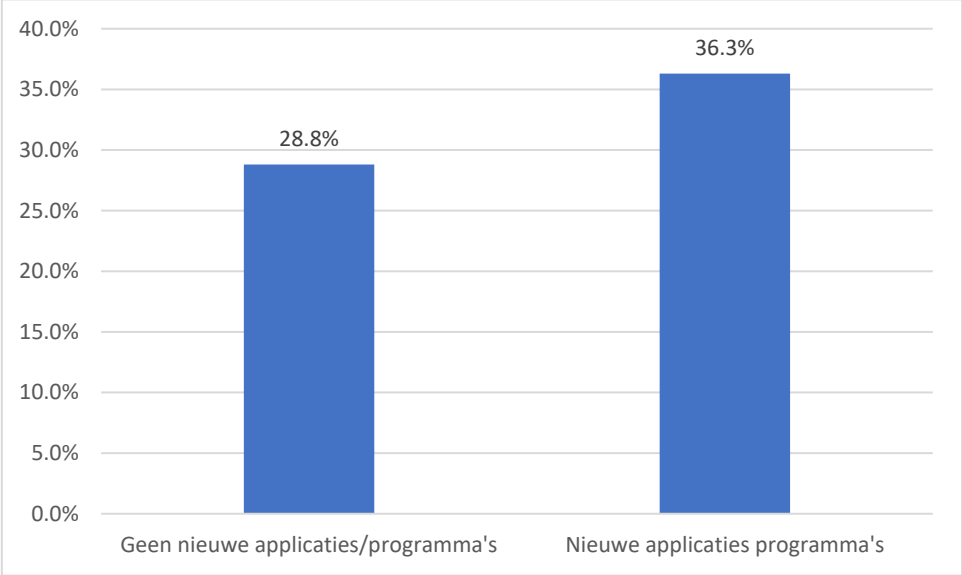
Figuur 8: Slachtofferschap cybercriminaliteit, opgesplitst naar verandering in privé internetgebruik



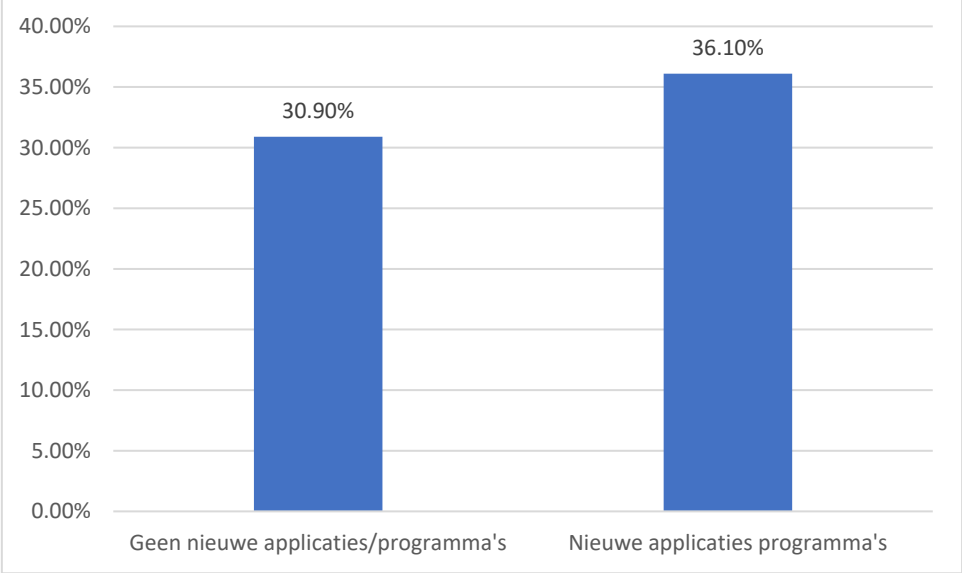
Tot slot zijn respondenten gevraagd of ze sinds de uitbraak van het coronavirus nieuwe applicaties of programma's hebben moeten gebruiken voor hun werkzaamheden op het werk of thuis. Figuur 9 en 10 tonen het verband aan tussen het gebruik van nieuwe applicaties en programma's en slachtofferschap van cybercriminaliteit. Uit Figuur 9 blijkt dat respondenten die op het werk nieuwe applicaties of programma's gebruiken significant ($p<.05$) vaker slachtoffer zijn geworden van cybercriminaliteit (36.3%) dan respondenten die dat niet hebben hoeven doen (28.8%). Ook respondenten die thuis voor hun werkzaamheden nieuwe applicaties of programma's hebben moeten gebruiken (36.1%) worden vaker

slachtoffer dan zij die dat niet hoefden (30.9%), al is dit verschil niet significant. De analyses uit Figuur 9 en 10 zijn ook apart uitgevoerd voor burgers en mkb'ers. Deze additionele analyses laten eenzelfde beeld zien voor beide groepen, maar geen van de resultaten is meer significant. Mogelijk komt dit door de verminderde statistische power na het opsplitsen van de steekproef.

Figuur 9: Slachtofferschap cybercriminaliteit, opgesplitst naar gebruik nieuwe applicaties en programma's op het werk



Figuur 10: Slachtofferschap cybercriminaliteit, opgesplitst naar gebruik nieuwe applicaties en programma's thuis



4. Discussie

In deze studie is onderzocht wat de invloed is geweest van de coronacrisis op de aard, omvang en gevolgen van cybercriminaliteit onder Nederlandse burgers en mkb'ers. Naast 10 kwalitatieve interviews met experts op het gebied van cyberveiligheid werd gebruik gemaakt van een panel van burgers en mkb'ers die in 2019 en/of 2021 zijn ondervraagd over onder andere hun slachtofferschap van, en angst voor, cybercriminaliteit. Hiermee is dit rapport de eerste studie waarin de invloed van de coronapandemie op zelf-gerapporteerd slachtofferschap van cybercriminaliteit in Nederland wordt onderzocht.

De resultaten van dit onderzoek laten zien dat er, onder zowel burgers als mkb'ers, slechts een kleine toename was van het aantal slachtoffers van cybercriminaliteit gedurende de pandemie in vergelijking met twee jaar eerder. Deze stijging was bovendien niet significant. Ook wanneer de 10 soorten cybercriminaliteit die in deze studie zijn meegenomen (i.e., malware, ransomeware, phishing, hacken, cyberstalking, identiteitsfraude, aan- en verkoopfraude, online dating fraude, online bedreigingen en DDoS-aanvallen) apart worden onderzocht, wordt voor de meeste delicten geen verandering in de prevalentie gevonden. Enkel online bedreigingen onder burgers en malware besmettingen onder mkb'ers namen significant af. Voor slachtofferschap van aan-en verkoopfraude wordt daarentegen een significante stijging gevonden onder zowel burgers als mkb'ers. Deze bevinding is in lijn met onderzoek uit het Verenigd Koninkrijk waar ook een stijging wordt gevonden in de prevalentie van aan-en verkoopfraude op basis van officiële registraties (Buil-Gil et al., 2021; Johnson & Nikolovska, 2022; Kemp et al., 2021). Het is echter belangrijk om op te merken dat de stijgingen in slachtofferschap van aan- en verkoopfraude in onze studie niet meer significant waren nadat alleen respondenten werden gereserveerd die in beide waves deelnamen. Dit kan er op duiden dat de stijging (deels) het gevolg was van een andere compositie van de steekproef in 2021 ten opzichte van 2019.

De bevinding dat slachtofferschap van cybercriminaliteit in het algemeen niet significant is toegenomen en dat sommige vormen van cybercriminaliteit zelfs zijn afgenomen gedurende de coronacrisis komt niet overeen met het meeste eerdere onderzoek naar dit onderwerp. Vrijwel alle studies op basis van officiële registraties vonden namelijk een toename van slachtofferschap van cybercriminaliteit gedurende de pandemie (Buil-Gil et al.,

2021; Buil-Gil & Zeng, 2022; Johnson & Nikolovska, 2022; Kemp et al., 2021; Kruisbergen et al., 2021). Studies op basis van zelfrapportages van slachtoffers (Hawdon et al., 2020) en daders (Weulen Kranenbarg et al., In druk), daarentegen, lieten in lijn met dit onderzoek geen verandering zien in de prevalentie van cybercriminaliteit. Deze discrepantie tussen gevonden trends in cybercriminaliteit in officiële registraties en in zelf-rapportages suggereert dat er niet zo zeer een toename is geweest van cybercriminaliteit tijdens de pandemie maar dat er een toename heeft plaatsgevonden in het melden en registreren van cybercriminaliteit. Ook in één van de kwalitatieve interviews gaf een expert aan dat hij/zij verwachtte dat mensen ten tijde van de pandemie sneller melding zou maken van cybercriminaliteit omdat ze meer thuis zaten. Daarnaast werd het in Nederland bijvoorbeeld vanaf april 2020 mogelijk om online aangifte te doen van vriend-in-nood-fraude, wat het mogelijk makkelijker maakte voor slachtoffers om naar de politie te stappen. Ook is het mogelijk dat men door de plotselinge overgang van veel offline activiteiten en werkzaamheden naar online varianten meer bewust is geworden van de risico's van online gedrag en dat men hierdoor eerder melding maakt van slachtofferschap bij officiële instanties. Zo blijkt uit ons onderzoek ook dat burgers significant meer angst hadden voor cybercriminaliteit, maar ondanks deze toegenomen angst was er dus geen sprake van een stijging van cybercriminaliteit gedurende de pandemie.

Alhoewel de resultaten van deze studie geen invloed laten zien in de omvang van cybercriminaliteit gedurende de coronapandemie, lijkt de modus operandi van de cybercriminelen wel verandert te zijn. Diverse experts gaven in de kwalitatieve interviews aan dat zij merkten dat aspecten van de coronacrisis onderdeel waren van de modus operandi, gedurende de pandemie. Ook uit de kwantitatieve analyses bleek dat een deel van de slachtoffers van elke vorm van cybercriminaliteit aangaf dat de daders bij het plegen van het delict misbruik maakten van de pandemie. Dit was met name vaak het geval bij de verschillende vormen van fraude (i.e. identiteitsfraude, aan- en verkoopfraude, online dating fraude), waar ongeveer een kwart van de slachtoffers aangaf dat dit het geval was. Dit resultaat toont aan dat het cybercriminele speelveld voortdurend aan verandering onderhevig is en dat cybercriminelen inspelen op de actualiteit om nieuwe mogelijkheden te ontwikkelen om slachtoffers te maken. Naidoo (2020) kwam tot eenzelfde conclusie na een content-analyse van documenten over 185 online fraude-gevallen. Het is dus van groot belang dat men in de bestrijding van cybercriminaliteit continue alert blijft op veranderingen

in de modus operandi van cybercriminelen, en rekening houdt met het feit dat zij misbruik maken van actuele maatschappelijke problemen.

Ondanks dat een aanzienlijk deel van de respondenten aangeeft slachtoffer te zijn geweest van cybercriminaliteit, lijkt de financiële schade in de meeste gevallen mee te vallen. Bij de meeste vormen van cybercriminaliteit (i.e., malware, online bedreigingen, DDoS aanvallen, hacking, cyberstalking, identiteitsfraude, en online dating fraude) gaf geen enkele of slechts één respondent aan financiële schade te hebben geleden, waarbij de bedragen varieerden tussen de 50 en 500 euro. Daarentegen waren er met name bij aan- en verkoopfraude wel veel respondenten met financiële schade, welke soms zelfs opliep tot duizenden euro's. Vanuit dit oogpunt is het dus wel problematisch dat met name dit type delict is toegenomen tijdens de pandemie, waardoor ook de totale financiële schade die werd geleden door cybercriminaliteit kan zijn toegenomen.

Enkele geïnterviewde experts uitten ook hun zorgen dat de grootschalige verandering naar thuiswerken de aanvalsmogelijkheden voor cybercriminelen deed toenemen, bijvoorbeeld omdat nieuwe applicaties voor videobellen en online vergaderen plotseling veelvuldig gebruikt werden. Ook uit de kwantitatieve analyses komt naar voren dat respondenten die tijdens de coronacrisis nieuwe applicaties en programma's moesten gebruiken voor hun werk significant vaker slachtoffer werden van cybercriminaliteit. Dit toont aan dat het belangrijk is dat werkgevers bij het gebruik van nieuwe applicaties en programma's zich ook bewust zijn van de risico's die dit met zich mee brengt en dat zij hun werknemers instructies geven om deze applicaties en programma's op een veilige manier te gebruiken.

Tot slot werd in dit onderzoek onderscheid gemaakt tussen burgers en mkb'ers, maar bleken de resultaten tussen deze twee groepen erg overeen te komen. Slachtofferschap van cybercriminaliteit in 2021 was bijvoorbeeld nagenoeg gelijk. Ook in eerder onderzoek werd gevonden dat resultaten voor burgers en mkb'ers veel overeenkomsten vertonen (Van de Weijer et al., 2020). Een mogelijke verklaring hiervoor is dat een aanzienlijk deel van de mkb'ers in deze studie zzp'er is en eerder onderzoek heeft aangetoond dat het internetgebruik van bijna alle zzp'ers in Nederland een mix is van privé- en zakelijk activiteiten (Veenstra et al., 2016). Hierdoor is het lastig om onderscheid te maken tussen slachtofferschap als persoon en als bedrijf. Desalniettemin suggereert de bevinding dat

burgers en mkb'ers even vaak slachtoffer werden, dat cybercriminelen het gedurende de coronacrisis niet specifiek op mkb'ers gemunt hadden.

4.1 Limitaties

Bij het interpreteren van de resultaten van deze studie is het van belang om enkele limitaties in ogenschouw te nemen. Ten eerste meet deze studie slachtofferschap van cybercriminaliteit op slechts twee momenten, in mei 2019 en april/mei 2021. In tegenstelling tot diverse studies op basis van officiële registraties, die doorgaans over een lange periode cijfers op wekelijks niveau hebben, is het daarom niet mogelijk om te onderzoeken of er voorafgaand aan de coronapandemie al sprake was van een stijgende of dalende trend in slachtofferschap van cybercriminaliteit. Indien er op de lange termijn bijvoorbeeld sprake zou zijn van een daling van slachtofferschap van cybercriminaliteit, kan de bevinding van dit rapport dat cybercriminaliteit niet is toegenomen tussen 2019 en 2021 er juist op wijzen dat de pandemie weldegelijk heeft geleid tot meer cybercriminaliteit. Gegevens over zelf-gerapporteerd slachtofferschap in de Veiligheidsmonitor van het CBS (2020) laten echter zien dat er geen sprake is van een afname van cybercriminaliteit in Nederland tussen 2012 en 2019, maar dat er eerder sprake is van een stijgende trend sinds 2016.[5] Dit sterkt onze conclusie dat er daadwerkelijk geen stijging in cybercriminaliteit heeft plaatsgevonden gedurende de coronacrisis.

Ten tweede werden de respondenten in deze studie gevraagd naar slachtofferschap van cybercriminaliteit gedurende het jaar voorafgaand aan april/mei 2021. Aangezien de eerste (intelligente) lockdown in Nederland plaatsvond tussen 16 maart 2020 en 31 mei 2020, is het begin van deze lockdown niet geheel meegenomen in de meting van slachtofferschap. Het is aannemelijk dat de grootste veranderingen in ons leven, werk en internet-gedrag plaatsvonden in de eerste weken van deze lockdown, waardoor mensen in die weken ook het meest kwetsbaar waren voor cybercrime-aanvallen. Kruisbergen en collega's (2021) laten inderdaad zien dat de stijging van geregistreerde cybercriminaliteit het hoogst is gedurende de eerste lockdown. Het uitblijven van een stijging van cybercriminaliteit in de resultaten van deze studie kan dus mogelijk het gevolg zijn van het feit dat slachtofferschap niet gemeten is

[5] De meest recente versie van de Veiligheidsmonitor (2022) meette zelf-gerapporteerd slachtofferschap van cybercriminaliteit in 2021. Helaas zijn de onderzoeksmethoden en vraagstelling in deze versie dermate verandert dat een vergelijking met eerder jaren onmogelijk is.

gedurende de eerste weken van de pandemie. Echter, mocht de prevalentie van cybercriminaliteit in deze eerste weken daadwerkelijk gestegen zijn, dan is er dus geen sprake geweest van een blijvend effect van de verandering van offline activiteiten en werkzaamheden naar online activiteiten en werkzaamheden. Een ander nadeel van het bevragen van slachtofferschap over een geheel jaar is dat er geen onderscheid gemaakt kan worden tussen slachtofferschap gedurende verschillende periodes, zoals (het eind van) de eerste 'intelligente lockdown' (16 maart - 31 mei 2020), de periode van versoepelingen (1 juni – 13 september 2020), de periode van beperkte maatregelen (14 september – 13 december 2020), en de tweede 'harde lockdown' (14 december 2020 – 14 maart 2021). Omdat de mate van offline en online activiteiten en werkzaamheden mogelijk nogal sterk verschilden tussen deze periodes, zou ook de prevalentie van cybercriminaliteit kunnen fluctueren. In het huidige onderzoek was dit dus helaas niet te meten.

Ten derde kan het zijn dat respondenten niet altijd weten of ze slachtoffer zijn geweest van cybercriminaliteit. Met name bij slachtofferschap van hacken of malware besmettingen kan het mogelijk zijn dat slachtoffers hier nooit achter komen. De prevalentie van deze soorten cybercriminaliteit is dus mogelijk hoger dan blijkt uit deze studie. Dit geldt echter zowel voor de metingen in 2019 en 2021, en heeft alleen invloed op de conclusies over (het uitblijven van) veranderingen in slachtofferschap gedurende de pandemie wanneer respondenten over tijd vaker op de hoogte zijn van hun slachtofferschap. Dit zou mogelijk kunnen zijn wanneer respondenten vaker antivirus software zijn gaan gebruiken, bijvoorbeeld omdat dat door hun werkgever verplicht werd toen ze tijdens lockdowns thuis moesten werken, en hierdoor meldingen ontvangen van (pogingen tot) aanvallen van cybercriminelen. In lijn met deze redenering laten onze resultaten inderdaad zien dat respondenten die nieuwe applicaties of programma's zijn gaan gebruiken ook vaker slachtoffer werden van cybercriminaliteit. Echter, blijkt uit onze resultaten ook dat de prevalentie van zowel malware als hacken is gedaald in 2021 ten opzichte van 2019 (al is deze daling in de meeste gevallen niet significant), wat juist suggereert dat deze nieuwe applicaties en programma's niet hebben geleid tot het eerder opmerken van deze soorten cybercriminaliteit.

Tot slot is het cybercriminele speelveld voortdurend aan verandering onderhevig en ontstaan er door technologische ontwikkelingen voortdurend nieuwe mogelijkheden om cybercriminaliteit te plegen. Een voorbeeld is Whatsapp-fraude, een specifieke vorm van

vriend-in-nood fraude die de laatste jaren veelvuldig voorkomt (Van ’t Hoff-de Goede & Leukfeldt, 2021). Om de vergelijking tussen 2019 en 2021 optimaal te houden, hebben we er in dit onderzoek voor gekozen om de vraagstelling, en dus de verschillende soorten cybercriminaliteit waar naar gevraagd werd, exact hetzelfde te houden. Een nadeel van dit besluit is dat we mogelijk nieuwere vormen van cybercriminaliteit, zoals Whatsapp-fraude, niet meten en dus ook niet meenemen in de totale prevalentie van cybercriminaliteit.

4.2 Conclusie

Concluderend laat deze studie zien dat slachtofferschap van cybercriminaliteit onder Nederlandse burgers en mkb’ers niet is toegenomen tijdens de coronacrisis. Het feit dat officiële registraties van cybercriminaliteit wel toenamen (zie bijv. Kruisbergen et al., 2021) suggereert dat slachtoffers wel vaker melding maken van hun slachtofferschap. Alhoewel geen toename in slachtofferschap van cybercriminaliteit wordt gevonden, is de coronapandemie wel degelijk van invloed geweest op cybercriminaliteit. Slachtoffers geven namelijk aan dat een aanzienlijk deel van de delicten corona-gerelateerd was, met name bij vormen van online fraude. Cybercriminelen lijken dus in te spelen op de actuele ontwikkelingen rondom de coronacrisis en hun modus operandi hierop aan te passen. Tot slot blijkt uit onze resultaten dat het gebruik van nieuwe applicatie en programma’s voor werk samenhangt met een verhoogd risico op slachtofferschap van cybercriminaliteit tijdens de coronacrisis.

5. Referenties

Agnew, R. (1992). Foundation for a General Strain Theory of Crime and Delinquency. *Criminology*, *30*(1), 47–88. https://doi.org/10.1111/j.1745-9125.1992.tb01093.x

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*, *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. *Journal of Financial Crime*, *29*(2), 460–475. https://doi.org/10.1108/JFC-02-2021-0042

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. *American Sociological Review*, *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. *Journal of Family 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. *Security Journal*, *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. *American Journal of Criminal Justice*, *45*(4), 546–562. https://doi.org/10.1007/s12103-020-09534-4

Johnson, S. D., & Nikolovska, M. (2022). *The effect of COVID-19 restrictions on routine activities and online crime* [Preprint]. SocArXiv. https://doi.org/10.31235/osf.io/ze49b

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. *Journal of Contemporary Criminal 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. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Leukfeldt, E.R. (2018) *De 'human' factor in cybersecurity* (inaugural speech). Den Haag: Haagse Hogeschool

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 Science*, *8*(1), 12. https://doi.org/10.1186/s40163-019-0107-y

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *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. *Nature Human Behaviour*, *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.

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. *American Journal of Criminal Justice*, *45*(4), 563–577. https://doi.org/10.1007/s12103-020-09532-6

Stickle, B., & Felson, M. (2020). Crime Rates in a Pandemic: The Largest Criminological Experiment in History. *American Journal of Criminal Justice*, *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.

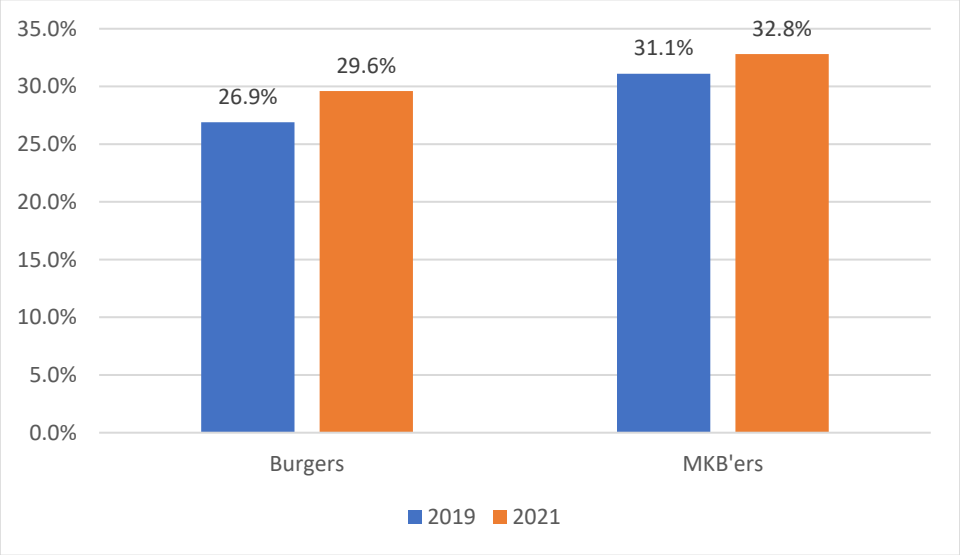
van 't Hoff-de Goede, S. & Leukfeldt, R. (2021) *WhatsAppfraude komt veelvuldig voor in Nederland*. CCV Secondant. https://ccv-secondant.nl/platform/article/whatsappfraude-komt-veelvuldig-voor-in-nederland

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*. Leeuwarden: Lectoraat Cybersafety.

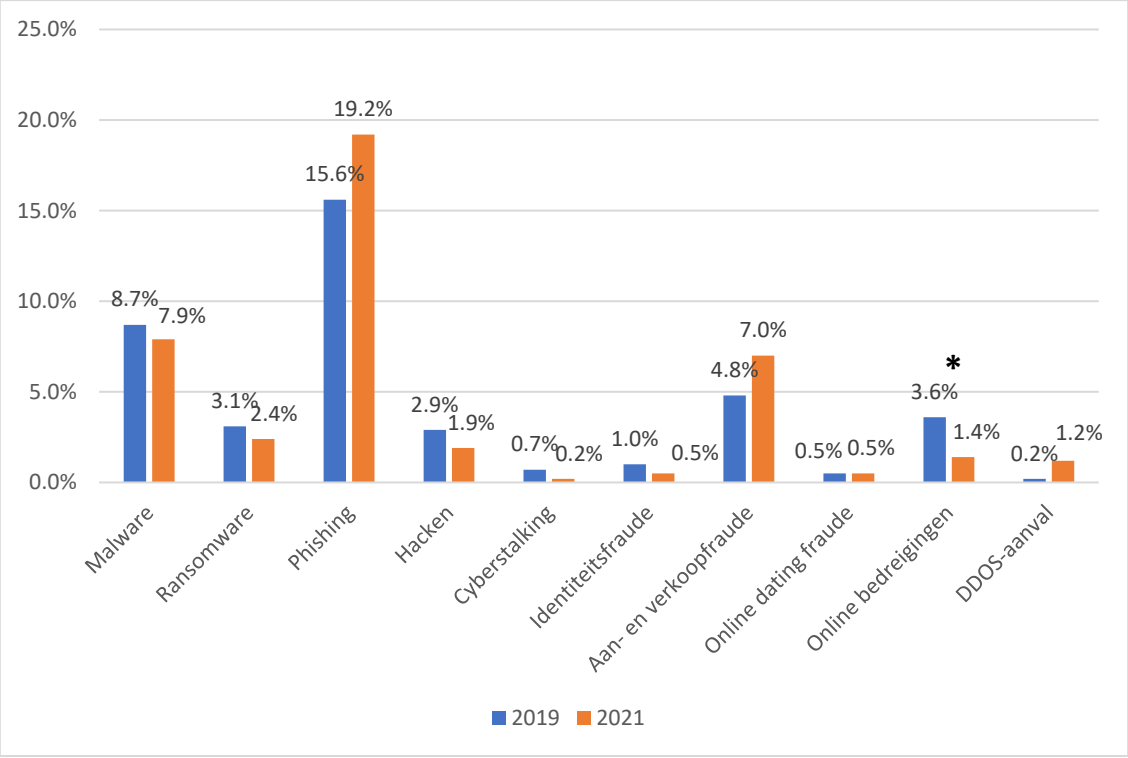
Weulen Kranenbarg, M. & Weerman, F. (In druk). *Online jeugdcriminaliteit in coronatijd: Ontwikkelingen in zelfgerapporteerd daderschap, activiteiten en contacten met vrienden bij een hoog risicogroep.*

Appendix: Resultaten respondenten die meededen aan beide waves

Figuur A1: Prevalentie cybercriminaliteit in 2019 en 2021

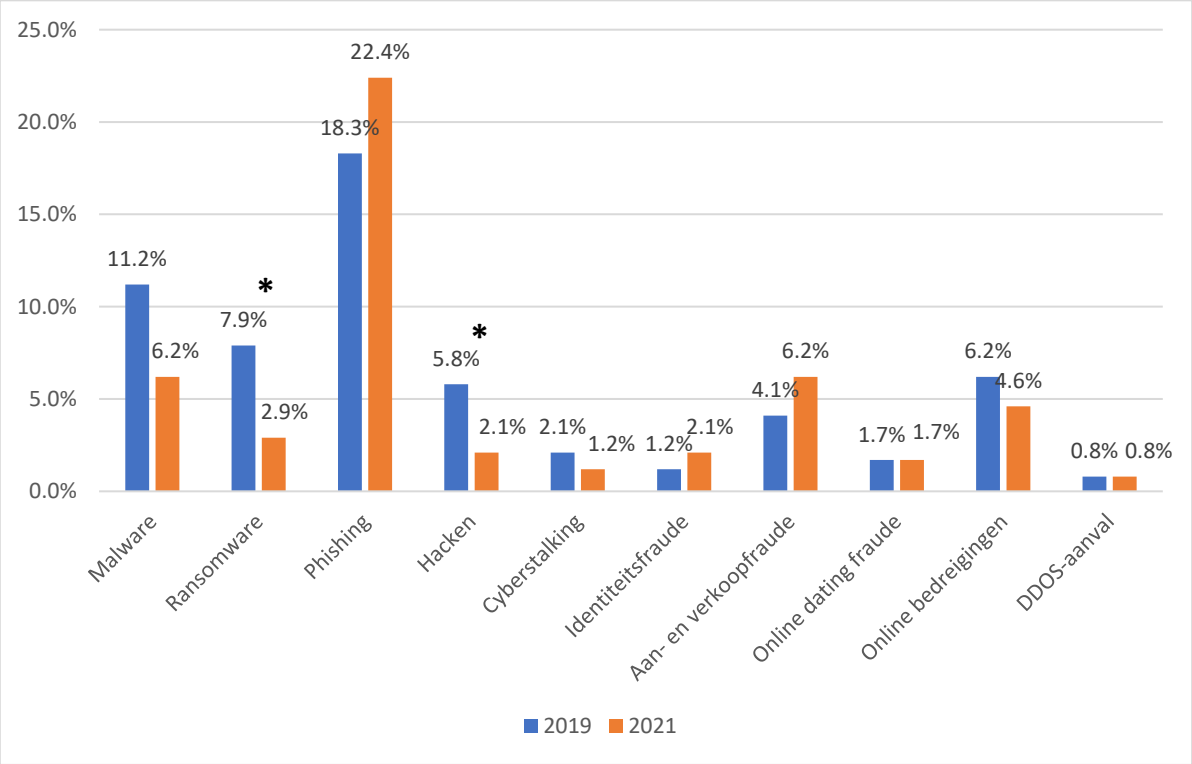


Figuur A2: Prevalentie 10 soorten cybercriminaliteit onder burgers, in 2019 en 2021



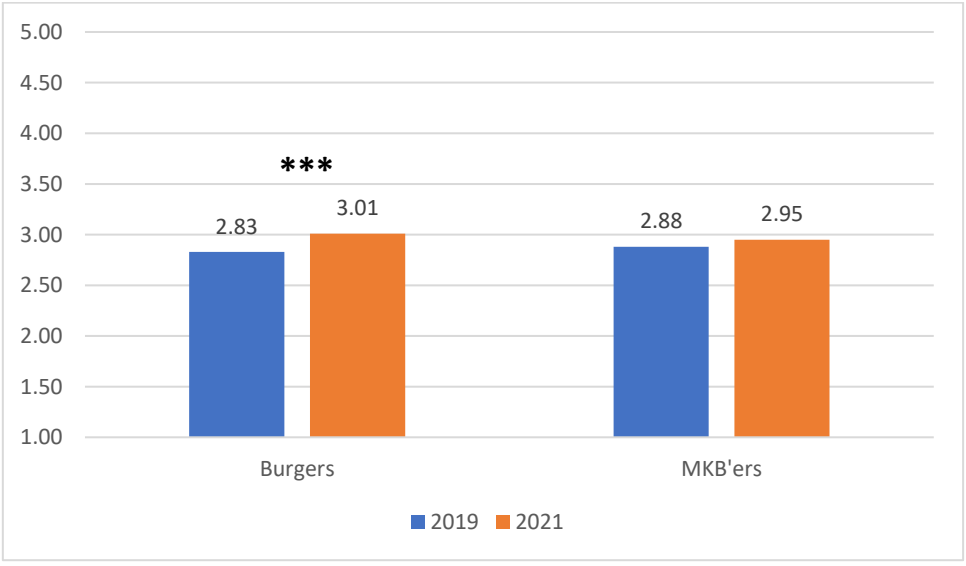
*Noot: *p<.05*

Figuur A3: Prevalentie 10 soorten cybercriminaliteit onder mkb'ers, in 2019 en 2021



*Noot: *p<.05*

Figuur A4: Angst voor cybercriminaliteit in 2019 en 2021



*Noot: ***p<.001*

Het NSCR is onderdeel van de institutenorganisatie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO)

Bezoekadres:
De Boelelaan 1077
1081 HV Amsterdam

Postadres:
Postbus 71304
1008 BH Amsterdam

T 020 598 5239
E nscr@nscr.nl
W www.nscr.nl

nscr

Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving