Nieuwsbrief september 2021

Middels deze maandelijkse nieuwsbrief van het Kennisnetwerk Victimologie in Nederland, brengen wij je graag op de hoogte van updates en activiteiten van ViNe, van haar netwerkleden, en van ander victimologisch nieuws. Ditmaal met het thema: slachtofferschap van cybercriminaliteit.

Hiervoor spraken wij Susanne van 't Hoff-de Goede, Rutger Leukfeldt en Madeleine van der Bruggen.

ViNe-netwerklid Susanne van 't Hoff-de Goede geeft ons uitleg over slachtofferschap van cybercriminaliteit:

Wat wordt verstaan onder cybercriminaliteit?

Onder cybercriminaliteit vallen delicten die doorgaans in twee categorieën worden ingedeeld. Nieuwe delicten vallen onder de noemer cybercrime. De meest voorkomende vormen zijn hacking en malware. Traditionele vormen van criminaliteit die zich inmiddels ook online afspelen vallen onder de noemer gedigitaliseerde criminaliteit. De meest voorkomende financiële delicten zijn phishing en aankoopfraude. Op interpersoonlijk gebied komen laster, chantage en stalking het vaakst voor. Ook ontstaat er voortdurend nieuwe vormen van cybercriminaliteit, zoals bijvoorbeeld WhatsApp-fraude. Uit een onderzoek dat wij deden onder een representatieve sample van de Nederlandse bevolking bleek dat ruim 15% van de Nederlandse volwassenen in 2020 een poging tot WhatsApp-fraude heeft meegemaakt. Zo'n 5% van hen maakte vervolgens geld over (0,7% van de populatie).

Wat is de prevalentie van slachtofferschap van cybercriminaliteit?

Slachtofferschap van cybercriminaliteit neemt al jaren toe en kan – net als voor traditionele vormen van slachtofferschap – grote impact hebben op slachtoffers. Recente studies onder grote groepen Nederlanders hebben laten zien dat zo'n 10-13% van de Nederlanders in het afgelopen jaar slachtoffer is geworden van een of meerdere cyberdelicten. Zelfs bij deze hoge prevalentie van slachtofferschap, moet rekening geworden houden met het feit dat deze cijfers een onvolledig beeld laten zien. Een reden hiervoor is bijvoorbeeld dat mensen niet altijd weten dat ze slachtoffer zijn, zoals in het geval van het stelen van persoonsgegevens en malware. Ook is de aangiftebereidheid laag.

Welke groepen worden het vaakst slachtoffer?

Op eerste oog mogelijk contra-intuïtief, worden jongeren vaker slachtoffer van cybercriminaliteit dan ouderen. Slachtoffers lijken nauwelijks te verschillen op andere kenmerken, zoals geslacht en opleiding. Enkele van onze lopende onderzoeksprojecten richten zich er dan ook op om slachtofferschap te verklaren vanuit online gedrag. Wanneer we weten hoe mensen zich online gedragen en hoe dit het risico op slachtofferschap beïnvloedt, kunnen we werken aan interventies om slachtofferschap van cybercriminaliteit terug te dringen.

ViNe nieuws

Jubileumsymposium

Dit najaar bestaat ViNe 1 jaar! Daarom wordt er op vrijdag 5 november 2021 weer een ViNe-symposium georganiseerd. Ditmaal met het thema, passend bij de huidige nieuwsbrief: 'Slachtoffers van schadelijk/crimineel gedrag online'. Houd onze informatiekanalen in de gaten voor nadere informatie. Mocht je je alvast willen aanmelden, dan kan dat via dit aanmeldformulier.

Netwerklid worden

Ook netwerklid worden? Aanmelden kan middels dit formulier.

Contactinformatie

victimologie.nl@gmail.com

http://www.victimologie.nl

Kennisnetwerk Victimologie in Nederland (ViNe)

Wat kunnen we de komende tijd op onderzoeksgebied van jou verwachten?

Samen met collega's werk ik aan onderzoeken binnen de "human factor" van cybercriminaliteit: daders, slachtoffers en handhavers. Zo loopt er momenteel een longitudinaal onderzoek naar de relatie tussen online gedrag en slachtofferschap, waarin we ook kijken naar factoren zoals kennis, motivatie, gelegenheid en zelfcontrole. Ook werken we aan een set wetenschappelijk onderbouwde interventies die gemeenten kunnen inzetten om de cyberweerbaarheid onder jongeren, ouderen en mkb'ers in hun regio te vergroten. Daarnaast ronden wij momenteel een onderzoek af naar projecten binnen de politie waarin op lokaal niveau de aanpak van cybercriminaliteit wordt bevorderd.

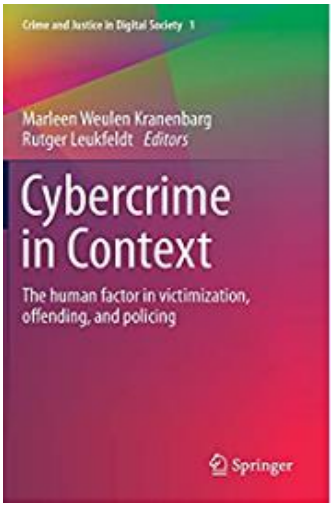
Recente initiatieven op het gebied van online slachtofferschap:

- Het Rathenau Instituut heeft een rapport gepubliceerd genaamd 'Online Ontspoord' over schadelijk en immoreel gedrag op het internet. Het rapport gaat onder andere in op het helpen voorkomen van online slachtofferschap en bevat aanbevelingen hoe slachtoffers te beschermen en bij te staan. Mariëtte van Huijstee komt er tijdens het symposium op 5 november meer over vertellen.

- Het Bureau Regionale Veiligheidsstrategie (RVS) Midden-Nederland deelt een podcastserie over digitale criminaliteit genaamd 'Digitaal Beroofd', waarin slachtoffers hun verhaal doen. Politie, OM en wetenschappers geven een kijkje achter de schermen van deze snelgroeiende vorm van criminaliteit.

- Een initiatief dat tevens om ervaringsverhalen van slachtoffers draait betreft 'Het slachtoffer spreekt', van Noord-Holland Samen Veilig. Burgers wordt opgeroepen hun verhaal omtrent cybercriminaliteit via dit verhalenplatform te delen, om zo meer bekendheid te generen over de werkwijze van cybercriminelen.

ViNe-netwerklid Rutger Leukfeldt, redacteur van het boek '*Cybercrime in context. The human factor in victimization, offending, and policing*', legt uit waarom dit boek voor victimologen interessant kan zijn:



Dit boek gaat over de menselijke factor in cybercriminaliteit: daders, slachtoffers en partijen die betrokken zijn bij de aanpak van cybercrime. Het boek biedt een divers internationaal perspectief op de reactie op en preventie van cybercriminaliteit, en kijkt daarbij zowel naar de technologische als de menselijke kant van cybercriminaliteit. Een aantal hoofdstukken zijn specifiek gericht op slachtofferschap van cybercriminaliteit. Zo is er een hoofdstuk over de impact van slachtofferschap van diverse cybercrimes, over het bestuderen van veilig en onveilig online gedrag van burgers, over de psychologie van een ransomware aanval, en over de rol die werknemers kunnen spelen bij incidenten binnen bedrijven.

Dit boek is met name interessant voor onderzoekers die zich bezig houden met (de psychologie van) cybercriminaliteit, evenals voor beleidsmakers en wetshandhavers die geïnteresseerd zijn in preventie en detectie.

Madeleine van der Bruggen is senior onderzoeker bij de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen. Daarnaast werkt ze aan een promotieonderzoek over netwerken van seksueel kindermisbruik op het Darkweb. In dit onderzoek werkt zij samen met Arjan Blokland (Universiteit Leiden, NSCR) en de Nationale Politie.

Voor deze nieuwsbrief licht ze haar werk bij de Nationaal Rapporteur toe, en vertelt ze over een analysemethode die ze heeft gebruikt in haar promotieonderzoek.

Meer informatie over Madeleine en recente publicaties van haar hand, is te vinden op Madeleine's netwerkledenpagina.

De Nationaal Rapporteur onderzoekt de aard en omvang van mensenhandel en seksueel geweld tegen kinderen en adviseert de overheid en professionals over het voorkomen en bestrijden hiervan. Uit onderzoek van de Nationaal Rapporteur blijkt dat daders steeds meer online opereren, en dat (mogelijke) slachtoffers online kwetsbaarder worden. De online en offline wereld zijn dus onlosmakelijk met elkaar verbonden.

Omdat het vergaren van kennis een belangrijke stap is in het beschermen van slachtoffers, doen we bij de Nationaal Rapporteur onderzoek naar online zedencriminaliteit en maken we daarbij gebruik van innovatieve onderzoekstechnieken. Hierbij werken we samen met andere partijen.

In één van de artikelen die onderdeel uitmaakt van mijn promotieonderzoek heb ik gebruik gemaakt van een unieke dataset om een dadertypologie van kinderpornodaders verder te ontwikkelen. In die set zat de volledige gespreksgeschiedenis van een Darkweb kinderpornoforum. Deze longitudinale data, lopend van december 2020 tot en met december 2014, is gebruikt als input voor het ontwikkelen van zogenaamde 'communicatie carrière trajecten', en met deze analyse zijn zes daderprofielen gedestilleerd. Zo bestaan er 'Lurkers', die het forum op een relatief laat moment betreden, vervolgens vrijwel geen forumactiviteit laten zien, en die het forum vervolgens ook weer snel verlaten. De kans is aanzienlijk dat zij hun criminele activiteiten zullen staken, wanneer bij hen het gevoel van pakkans toeneemt. Een ander voorbeeld van een van de profielen, is de groep 'Escalators', die een bovengemiddelde bijdrage aan het forum levert, vaak een hogere positie binnen het forum kent, en bij wie bovendien de frequentie van posten gedurende de tijd toeneemt. De kans op het staken van de criminele activiteiten is bij deze groep een stuk kleiner.

Deze resultaten zijn waardevol voor de opsporingspraktijk, omdat ze door de politie gebruikt kunnen worden in het prioriteren van bepaalde (groepen) daders. Daarnaast zijn verschillende typen Darkweb kinderpornodaders mogelijk vatbaar voor verschillende typen interventies om hen te behoeden voor recidive. Bovendien is het vergroten van kennis over dadergedrag essentieel voor de preventie van (toekomstig) daderschap en daarmee ook voor de preventie van (toekomstig) slachtofferschap. Zonder oog voor de daders blijven kinderen namelijk altijd kwetsbaar.

Meer over dit onderzoek is te lezen via:
Van der Bruggen, M., & Blokland, A. (2021). Profiling darkweb child sexual exploitation material forum members using longitudinal posting history data. *Social Science Computer Review*, https://doi.org/10.1177/0894439321994894

Suggesties voor de nieuwsbrief?
Neem contact met ons op!