Naar een *gefundeerde* aanpak van online criminaliteit

Handvatten voor praktische aanpakken op basis van wetenschappelijke en praktijkgerichte literatuur, interventies en praktische inzichten over daders en slachtoffers van online criminaliteit

Thijs van Beek MSc[1], Elmira Land BA[1], Joeri Loggen MSc[2], dr. Remco Spithoven[1] & prof. dr. Rutger Leukfeldt[2, 3, 4]

[1] Hogeschool Saxion, lectoraat Online Weerbaarheid.
[2] de Haagse Hogeschool, lectoraat Cybercrime & Cybersecurity.
[3] Nederlands Studiecentrum Criminaliteit en Rechtshandhaving.
[4] Universiteit Leiden, leerstoel Governing Cybercrime.

INLEIDING

Professionals in de praktijk zijn op zoek naar handvatten om dader- en slachtofferschap van online criminaliteit tegen te gaan. En dat is hard nodig. Al ruim tien jaar op rij worden jaarlijks twee miljoen inwoners van 15 jaar en ouder het slachtoffer van online criminaliteit (CBS, 2024). Naar schatting wordt ook jaarlijks een op de vijf mkb-ers slachtoffer van een cyberaanval (ENISA, 2021). Dit leidt tot grote impact onder de slachtoffers maar ook tot grote, maatschappelijke schade (Spithoven, 2020).

Voor veel professionals is criminaliteit in de online wereld ‘erbij’ gekomen. Hoewel er een stevige daling in de offline criminaliteit zichtbaar is geworden in de afgelopen twee decennia, hebben professionals hier in de praktijk hun handen evengoed nog aan vol. Er blijft ondanks de *crimedrop* meer offline criminaliteit plaatsvinden dan zij kunnen aanpakken (Spithoven, 2020). En hier is online criminaliteit in ingrijpende omvang en impact bijgekomen. Daarbij kan inmiddels worden gesproken van zowel *high volume* als *high impact crime* (Leukfeldt, 2024). Er wordt dan ook landelijk, regionaal en lokaal steeds meer prioriteit gegeven aan het tegengaan van online dader- en slachtofferschap door de politie en haar partners in de *politiefunctie*.

Voordat professionals zich op de praktische aanpak van online criminaliteit richten, moeten zij doorgaans een drempel over: deze vormen van criminaliteit worden vaak als ‘complex’ en ‘ technisch’ gezien. Voorbij deze *digitale koudwatervrees* (Spithoven & Leukfeldt 2023) blijkt veel van het werk doorgaans vergelijkbaar met de aanpak van criminaliteit in de offline wereld. In de *hybride* realiteit van criminaliteit vandaag de dag, is het echt nodig meters te gaan maken.

In dit rapport brengen wij - in opdracht van de agenda Digitalisering & Cybercrime van de Nationale Politie - verslag uit van onze gestructureerde zoektocht naar gefundeerde, praktische handvatten voor de praktijk op basis van wetenschappelijke en praktijkgerichte literatuur over daders en slachtoffers van online criminaliteit. In dit rapport presenteren wij onze bevindingen van (I) een gestructureerde, narratieve literatuurstudie van wetenschappelijke literatuur over dader- en slachtofferschap tussen 2013 en 2023, (II) een focusgroep onder ervaren professionals, (III) een scoping literatuurstudie van wetenschappelijke literatuur over daderschap tussen 2021 en 2024 en (IV) een scoping literatuurstudie van de beschikbare, praktijkgerichte literatuur over dader- en slachtofferschap. Hierbij zijn ook **interventies** meegenomen en, waar van toepassing, resultaten van evaluaties opgenomen.

Daarmee willen wij de politie en haar partners helpen om tot een ***gefundeerde* aanpak van dader- en slachtofferschap van online criminaliteit** te komen. Want veel professionals werken momenteel op eigen inzichten en heuristieken (Leukfeldt, 2024) en hebben logischerwijs niet de tijd zich in alle, beschikbare literatuur te verdiepen. Daar helpen wij vanuit Cyberweerbaar NL graag een academisch handje bij!

U kunt via de **overkoepelende inhoudsopgave** op de volgende pagina zoeken wat u nodig heeft, daarna volgen nog **inhoudsoverzichten voor dader- en slachtofferschap**. Daarbij vindt u steeds **totaaloverzichten** en **overzichten per delictstype**, zodat u desgewenst snel met de specifieke informatie aan de slag kan.

INHOUDSOPGAVE

Deze eindrapportage is opgedeeld in een zestal hoofdstukken die elk een deel van het onderzoek belichten.

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

OVERZICHT VAN ONDERWERPEN

DELICTSTYPEN MET BETREKKING TOT DADERSCHAP

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

→ Of: volg de eindrapportage op volgorde

Risicofactoren online criminaliteit – totaaloverzicht		
Risicofactoren per delictstype:		
Cybercrime in enge zin	Malware	Strafbare vormen van sexting
Hacking	Cyberstalking	
Inzichten uit de praktijk m.b.t. risicofactoren – totaaloverzicht		
Inzichten uit de praktijk m.b.t. risicofactoren per delictstype:		
Online criminaliteit, overkoepelend	Malware	Online fraude
Cybercrime in enge zin	Strafbare vormen van sexting	
Cyberstalking	Hacking	
Inzichten uit de wetenschap – totaaloverzicht		
Samenvatting inzichten uit de wetenschap – per delictstype:		
Online criminaliteit, overkoepelend	Online fraude	Bitcoin gerelateerde online criminaliteit
Cybercrime in enge zin	Geldezels	
Phishing/vishing	Social engineering	

Inzichten uit de wetenschap per delictstype:		
Hacking	Pig-butchering scam	Online bankpasfraude
Malware	Advance fee fraud	Social engineering
Online fraude	E-commerce fraude	Geldezels
Phishing	Concession-Abuse-as-a-Servive (CAaaS)-fraude	Bitcoin gerelateerde online criminaliteit
Vishing	Online werkgelegenheids-fraude	Overig
Datingfraude	Online werknemersfraude	
Inzichten over interventies uit de praktijkgerichte literatuur – totaaloverzicht		
Inzichten over **interventies** uit de praktijkgerichte literatuur per delictstype:		
Algemene weerbaarheid	Online geweld/ cyberpesten	Overig
Hacking + mal-/ransomware	Phishing	
Online fraude	Sexting/sextortion/ grooming	
Overkoepelende inzichten uit alle onderzoeken		
Overkoepelende inzichten per delictstype		

OVERZICHT VAN ONDERWERPEN

DELICTSTYPEN MET BETREKKING TOT SLACHTOFFERSCHAP

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

→ Of: volg de eindrapportage op volgorde

Risicofactoren online criminaliteit – totaaloverzicht	
Risicofactoren per delictstype:	
Online fraude	Phishing
Datingfraude	Fear of cybercrime
Inzichten uit de praktijk m.b.t. risicofactoren – totaaloverzicht	
Inzichten uit de praktijk m.b.t. risicofactoren per delictstype:	
Online criminaliteit, overkoepelend	Datingfraude
Online fraude	Phishing
Inzichten over interventies uit de praktijkgerichte literatuur – totaaloverzicht	
Inzichten over **interventies** uit de praktijkgerichte literatuur per delictstype:	
Algemene weerbaarheid	Online geweld/cyberpesten
Hacking + mal-/ransomware	Phishing
Online fraude	Sexting/sextortion/grooming
	Overig
Overkoepelende inzichten uit alle onderzoeken	
Overkoepelende inzichten per delictstype	

Afbeelding: Unsplash. (2024, 22 november). https://unsplash.com/photos/a-stack-of-books-sitting-on-top-of-a-table-0f6aNBub5t4

HOOFDSTUK 1

Resultaten systematische, narratieve review: risicofactoren voor dader- en slachtofferschap van online criminaliteit (2013 - 2023)

Joeri Loggen MSc.[1], Thijs van Beek MSc.[2], dr. Remco Spithoven[2] & prof. dr. Rutger Leukfeldt[1]

[1] de Haagse Hogeschool, lectoraat Cybercrime & Cybersecurity
[2] Hogeschool Saxion, lectoraat Online Weerbaarheid

OPBOUW HOOFDSTUK

HOOFDSTUK 1: RESULTATEN SYSTEMATISCHE REVIEW

Risicofactoren voor dader- en slachtofferschap van online criminaliteit

1.1: Toelichting vooraf

1.2: Overzicht per delictstype – daderschap

- 1.2.1: Cybercrime in enge zin
- 1.2.2: Hacking
- 1.2.3: Malware
- 1.2.4: Cyberstalking
- 1.2.5: Strafbare vormen van sexting

1.3: Totaaloverzicht risicofactoren – daderschap

1.4: Overzicht per delictstype – slachtofferschap

- 1.4.1: Online fraude
- 1.4.2: Datingfraude
- 1.4.3: Phishing
- 1.4.4: Fear of cybercrime

1.5: Totaaloverzicht risicofactoren – slachtofferschap

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

↩ Terug naar de inhoudsopgave

1.1 TOELICHTING VOORAF

In dit hoofdstuk wordt de systematische, narratieve review naar risicofactoren voor dader- en slachtofferschap van online criminaliteit op hoofdlijnen besproken. Hiervoor is in zes wetenschappelijke databases gezocht naar eerdere – **tussen 1 januari 2013 en 1 augustus 2023** gepubliceerde - gestructureerde literatuurstudies. Het omvangrijke deelrapport is via de link als pdf-bestand te downloaden.

Op de hierop volgende pagina's worden de resultaten uit dit onderzoek beknopt weergegeven. In dit onderzoek worden de risicofactoren besproken voor de volgende delictstypen;

Voor **daderschap**:
- Cybercrime in enge zin;
- Hacking;
- Malware;
- Cyberstalking;
- Strafbare vormen van sexting.

En voor **slachtofferschap**:
- Online fraude;
- Datingfraude;
- Phishing;
- Fear of cybercrime.


Risicofactoren voor dader- en slachtofferschap van online criminaliteit en de effectiviteit van interventies: Een systematische narratieve review

Joeri Loggen MSc.[1], Thijs van Beek MSc.[2], dr. Remco Spithoven[2] & prof.dr. Rutger Leukfeldt[1234]

[1] De Haagse Hogeschool, Centre of Expertise Cyber Security, Johanna Westerdijkplein 75, 2521 EN Den Haag.
[2] Saxion Hogeschool, Centrum voor Veiligheid en Digitalisering, Wapenrustlaan 11, 7321 DL Apeldoorn.
[3] Universiteit Leiden, Leerstoel Governing Cybercrime, Faculteiten Governance and Global Affairs & Rechtsgeleerdheid.
[4] Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving, De Boelelaan 1077, 1081 HV Amsterdam

PDF

Afbeelding betreft een screenshot van het voorblad van: Loggen, J., van Beek, T., Spithoven, R., & Leukfeldt, R. (2024). Risicofactoren voor dader- en slachtofferschap van online criminaliteit: een systematische, narratieve review. Cyberweerbaar NL.

↩ Terug naar de overzichtspagina van dit hoofdstuk

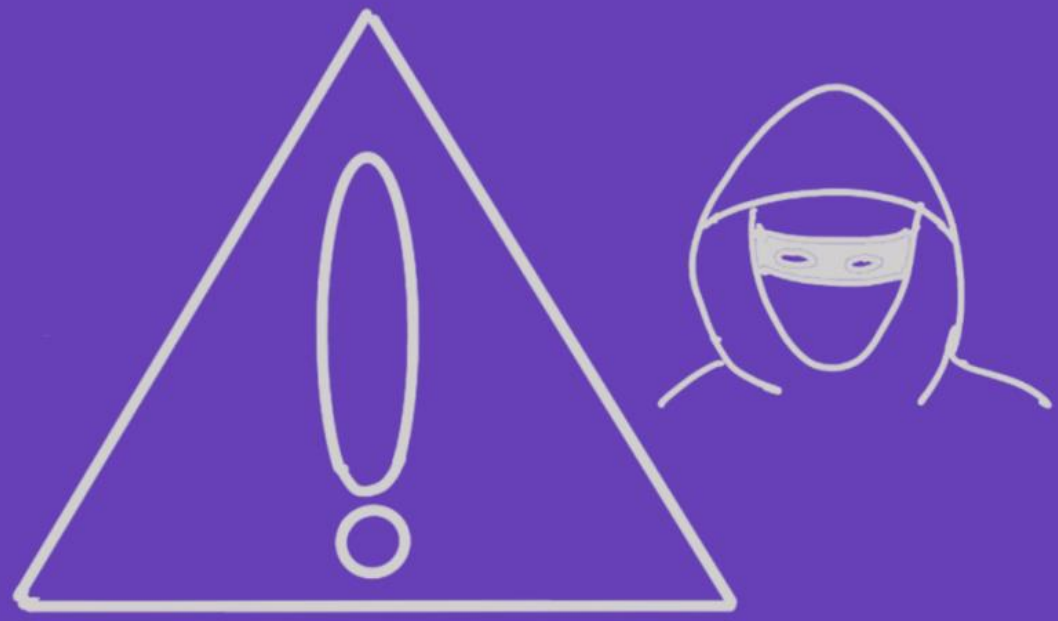
De risicofactoren worden op basis van een zevental categorieën weergegeven in tabellen. Deze categorieën zijn:

Demografische kenmerken:	Factoren als geslacht, leeftijd en opleidingsniveau.
Intrinsieke en persoonlijkheids-kenmerken:	Factoren als middelengebruik/verslaving, IT-kennis en zelfcontrole.
Mentaal:	Mentale aspecten zoals angst, depressie en geheugenproblemen.
Sociale relaties:	Factoren als eenzaamheid, band met ouders en deviante vrienden.
Routine activiteiten:	Factoren zoals internetgebruik en online activiteiten.
Criminaliteit:	Eerder slachtoffer- en/of daderschap.
Macrofactoren:	Factoren zoals schaamte, stigma, corruptie en cultuur.

De risicofactoren uit de hiernaast weergegeven categorieën zijn in het onderzoek ingedeeld op basis van de relatie ervan tot slachtoffer- of daderschap. Er zijn hierbij steeds drie verschillende relaties mogelijk, die ook in deze eindrapportage zullen worden gebruikt om de resultaten weer te geven. Dit zijn factoren met een:

1. **positieve** relatie: Hoe meer iemand dit kenmerk heeft of dit gedrag vertoont, hoe *groter* de kans dat hij of zij dader of slachtoffer wordt;
2. **negatieve** relatie: Hoe meer iemand dit kenmerk heeft of dit gedrag vertoont, hoe *kleiner* de kans dat hij of zij dader of slachtoffer wordt;
3. **ambigue** relatie: het is onduidelijk wat de invloed van dit kenmerk of dit gedrag is op dader- of slachtofferschap.

↩ Terug naar de overzichtspagina van dit hoofdstuk



PARAGRAAF 1.2

Risicofactoren daderschap online criminaliteit

Overzicht per delictstype

1.2.1 RISICOFACTOREN ONLINE CRIMINALITEIT

DADERSCHAP | Risicofactoren cybercrime in enge zin

RISICOFACTOREN | DADERSCHAP | CYBERCRIME IN ENGE ZIN		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Demografische kenmerken -	**Demografische kenmerken** ▪ Leeftijd	**Demografische kenmerken** ▪ Geslacht (man) ▪ Werk
Intrinsieke en persoonlijkheidskenmerken ▪ Autismespectrumstoornis (ASS) gerelateerde kenmerken ▪ Motivatie ▪ Zelfcontrole	**Intrinsieke en persoonlijkheidskenmerken** -	**Intrinsieke en persoonlijkheidskenmerken** -
Sociale relaties ▪ Deviante vrienden en social learning	**Sociale relaties** -	**Sociale relaties** -
Routine activiteiten ▪ Gaming	**Routine activiteiten** -	**Routine activiteiten** -

↩ Terug naar de overzichtspagina van dit hoofdstuk

1.2.2 RISICOFACTOREN ONLINE CRIMINALITEIT

DADERSCHAP | Risicofactoren hacking

RISICOFACTOREN | DADERSCHAP | HACKING		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Demografische kenmerken ▪ Geslacht (man) ▪ Opleidingsniveau ▪ Sociaal Economische Status	**Demografische kenmerken** ▪ Leeftijd	**Demografische kenmerken** ▪ Andere etniciteit (non-Kaukasisch) ▪ Werk
Intrinsieke en persoonlijkheidskenmerken ▪ Middelengebruik/verslaving ▪ Motivatie ▪ Neutralisatietechnieken	**Intrinsieke en persoonlijkheidskenmerken** ▪ Moraliteit ▪ Zelfcontrole	**Intrinsieke en persoonlijkheidskenmerken** ▪ Autismespectrumstoornis (ASS) gerelateerde kenmerken ▪ IT en computer kennis & vaardigheden ▪ Persoonlijkheidskenmerken
Sociale relaties ▪ Deviante vrienden en social learning	**Sociale relaties** ▪ Ouderlijk toezicht	**Sociale relaties** ▪ Band met ouders ▪ Sociale banden
Routine activiteiten ▪ Computer- en internetgebruik	**Routine activiteiten** -	**Routine activiteiten** -
Criminaliteit ▪ Daderschap overige online delicten	**Criminaliteit** -	**Criminaliteit** -

↩ Terug naar de overzichtspagina van dit hoofdstuk

1.2.3 RISICOFACTOREN ONLINE CRIMINALITEIT

DADERSCHAP | Risicofactoren malware

RISICOFACTOREN | DADERSCHAP | MALWARE		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Demografische kenmerken -	**Demografische kenmerken** -	**Demografische kenmerken** ▪ Geslacht (man)
Intrinsieke en persoonlijkheidskenmerken ▪ Autismespectrumstoornis (ASS) gerelateerde kenmerken ▪ IT en computer kennis & vaardigheden ▪ Neutralisatietechnieken	**Intrinsieke en persoonlijkheidskenmerken** ▪ Persoonlijkheidskenmerken	**Intrinsieke en persoonlijkheidskenmerken** -
Mentaal -	**Mentaal** ▪ Cognitieve vaardigheden	**Mentaal** -
Sociale relaties ▪ Deviante vrienden en social learning	**Sociale relaties** -	**Sociale relaties** -
Routine activiteiten -	**Routine activiteiten** -	**Routine activiteiten** ▪ Online routine activiteiten

↩ Terug naar de overzichtspagina van dit hoofdstuk

1.2.4 RISICOFACTOREN ONLINE CRIMINALITEIT

DADERS | Cyber-stalking

DADERSCHAP | Risicofactoren cyberstalking

RISICOFACTOREN | DADERSCHAP | CYBERSTALKING		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Demografische kenmerken ▪ Etniciteit ▪ Geslacht (man) ▪ Opleidingsniveau	**Demografische kenmerken** -	**Demografische kenmerken** -
Intrinsieke en persoonlijkheidskenmerken ▪ Middelengebruik/verslaving ▪ Persoonlijkheidskenmerken ▪ Risicogedrag	**Intrinsieke en persoonlijkheidskenmerken** -	**Intrinsieke en persoonlijkheidskenmerken** -
Mentaal ▪ Geestelijke gezondheidsproblemen	**Mentaal** -	**Mentaal** -
Sociale relaties ▪ Deviante vrienden en social learning	**Sociale relaties** ▪ Hechtingsproblemen ▪ Sociale steun	**Sociale relaties** -
Routine activiteiten ▪ Computer- en internetgebruik	**Routine activiteiten** -	**Routine activiteiten** -
Criminaliteit ▪ Daderschap offline criminaliteit ▪ Daderschap online criminaliteit ▪ Eerder slachtofferschap	**Criminaliteit** -	**Criminaliteit** -
Macrofactoren -	**Macrofactoren** -	**Macrofactoren** ▪ Cultuur

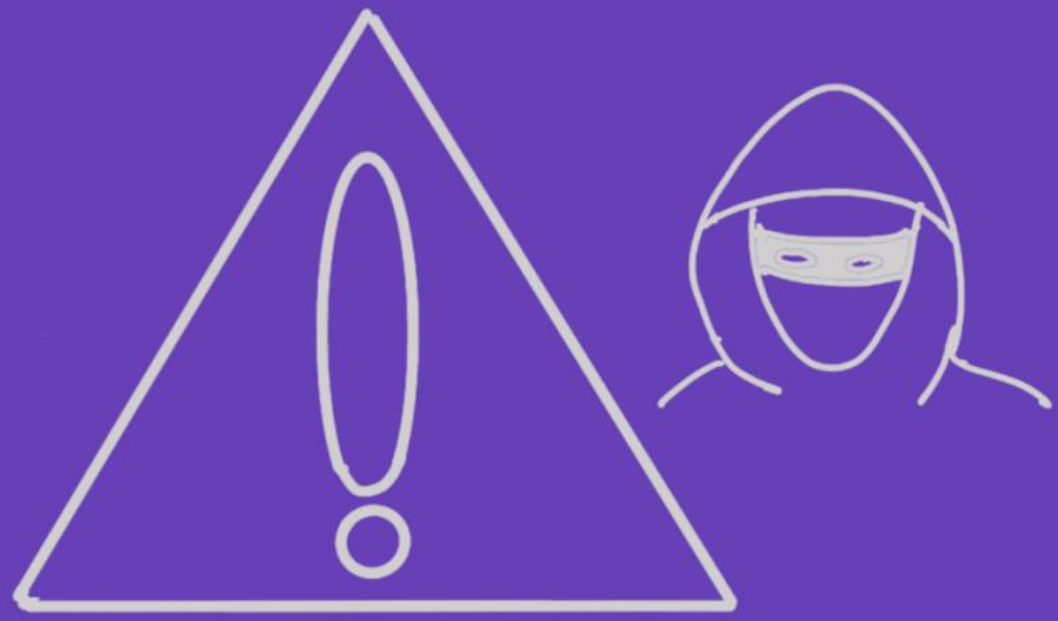
↩ Terug naar de overzichtspagina van dit hoofdstuk

1.2.5 RISICOFACTOREN ONLINE CRIMINALITEIT

DADERSCHAP | Risicofactoren strafbare vormen van sexting

RISICOFACTOREN | DADERSCHAP | STRAFBARE VORMEN VAN SEXTING		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Demografische kenmerken ▪ Geslacht (man) ▪ Opleidingsniveau	**Demografische kenmerken** -	**Demografische kenmerken** -
Intrinsieke en persoonlijkheidskenmerken ▪ Houding ten opzichte van sexting	**Intrinsieke en persoonlijkheidskenmerken** ▪ Persoonlijkheidskenmerken	**Intrinsieke en persoonlijkheidskenmerken** -
Sociale relaties -	**Sociale relaties** -	**Sociale relaties** ▪ Groepsdruk en peergroep

↩ Terug naar de overzichtspagina van dit hoofdstuk



PARAGRAAF 1.3

Bevindingen: risicofactoren daderschap online criminaliteit

Totaaloverzicht

1.3 RISICOFACTOREN ONLINE CRIMINALITEIT

DADERSCHAP | Risicofactoren totaaloverzicht

RISICOFACTOREN | DADERSCHAP | TOTAALOVERZICHT		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Demografische kenmerken ▪ Opleidingsniveau ▪ Geslacht (man)	**Demografische kenmerken** ▪ Leeftijd	**Demografische kenmerken** ▪ Geslacht
Intrinsieke en persoonlijkheidskenmerken ▪ Autismespectrumstoornissen gerelateerde kenmerken ▪ Middelengebruik/verslaving ▪ Risico's nemen ▪ Motivaties ▪ Neutralisatietechnieken	**Intrinsieke en persoonlijkheidskenmerken** -	**Intrinsieke en persoonlijkheidskenmerken** -
Sociale relaties ▪ Deviante vrienden en *social learning*	**Sociale relaties** -	**Sociale relaties** -
Routine activiteiten ▪ Computer- en internetgebruik	**Routine activiteiten** -	**Routine activiteiten** -
Criminaliteit ▪ Daderschap online criminaliteit	**Criminaliteit** -	**Criminaliteit** -

↩ Terug naar de overzichtspagina van dit hoofdstuk

PARAGRAAF 1.4

Bevindingen: risicofactoren slachtofferschap online criminaliteit

Overzicht per delictstype

1.4.1 RISICOFACTOREN ONLINE CRIMINALITEIT

SLACHTOFFERSCHAP | Risicofactoren online fraude | 1/2

RISICOFACTOREN | SLACHTOFFERSCHAP | ONLINE FRAUDE		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Demografische kenmerken ▪ Bezittingen	**Demografische kenmerken** -	**Demografische kenmerken** ▪ Inkomen ▪ Leeftijd ▪ Opleidingsniveau
Intrinsieke en persoonlijkheidskenmerken ▪ Autoriteit en legitimiteit ▪ Depressie ▪ Eenvoudige oplossingen ▪ Impulsiviteit ▪ Persoonlijkheidskenmerken ▪ Schaamte ▪ Vaardigheden digitale veiligheid ▪ Vertrouwen in autoriteit	**Intrinsieke en persoonlijkheidskenmerken** ▪ Bewustzijn ▪ Cognitieve vaardigheden ▪ IT-kennis	**Intrinsieke en persoonlijkheidskenmerken** ▪ Fysieke gezondheid ▪ Vertrouwen in anderen
Mentaal ▪ Geheugenproblemen	**Mentaal** ▪ Cognitieve functies	**Mentaal** -

1/2

↩ Terug naar de overzichtspagina van dit hoofdstuk

1.4.1 RISICOFACTOREN ONLINE CRIMINALITEIT

SLACHTOFFERSCHAP | Risicofactoren online fraude | 2/2

RISICOFACTOREN | SLACHTOFFERSCHAP | ONLINE FRAUDE		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Sociale relaties ▪ Eenzaamheid ▪ Isolement	**Sociale relaties** ▪ Partner	**Sociale relaties** -
Routine activiteiten ▪ Internetgebruik	**Routine activiteiten** ▪ Technologische toegang	**Routine activiteiten** -
Criminaliteit -	**Criminaliteit** ▪ Eerder slachtofferschap	**Criminaliteit** -
Macrofactoren ▪ Schaamte ▪ Stigma	**Macrofactoren** -	**Macrofactoren** -

INTERVENTIES | SLACHTOFFERSCHAP | ONLINE FRAUDE		
Opkomend/aanbeveling	**Niet opkomend/geen aanbeveling**	**Onduidelijk**
Interventies -	**Interventies** ▪ Bewustwording ▪ Weerbaarheid	**Interventies** -

2/2

↩ Terug naar de overzichtspagina van dit hoofdstuk

1.4.2 RISICOFACTOREN ONLINE CRIMINALITEIT

SLACHTOFFERSCHAP | Risicofactoren datingfraude

RISICOFACTOREN | SLACHTOFFERSCHAP | DATINGFRAUDE		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Demografische kenmerken ▪ Geslacht (vrouw) ▪ Opleidingsniveau	**Demografische kenmerken** -	**Demografische kenmerken** -
Intrinsieke en persoonlijkheidskenmerken ▪ Impulsiviteit	**Intrinsieke en persoonlijkheidskenmerken** ▪ Zelfcontrole ▪ Bewustzijn	**Intrinsieke en persoonlijkheidskenmerken** ▪ Neuroticisme ▪ Sensatiezucht

TRAININGEN & BEVEILIGINGSMAATREGELEN | SLACHTOFFERSCHAP | DATINGFRAUDE		
Opkomend/aanbeveling	**Niet opkomend/geen aanbeveling**	**Onduidelijk**
Trainingen & beveiligingsmaatregelen -	**Trainingen & beveiligingsmaatregelen** ▪ Profielherkenning ▪ Individuele strategie	**Trainingen & beveiligingsmaatregelen** -

↩ Terug naar de overzichtspagina van dit hoofdstuk

1.4.3 RISICOFACTOREN ONLINE CRIMINALITEIT

SLACHTOFFERSCHAP | Risicofactoren phishing | 1/2

RISICOFACTOREN | SLACHTOFFERSCHAP | PHISHING		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Demografische kenmerken -	**Demografische kenmerken** -	**Demografische kenmerken** ▪ Geslacht ▪ Leeftijd ▪ Etniciteit
Intrinsieke en persoonlijkheidskenmerken ▪ Autoriteit ▪ Heuristieken ▪ Impulsiviteit ▪ Persoonlijkheidskenmerken ▪ Zelfvertrouwen & zelfgenoegzaamheid	**Intrinsieke en persoonlijkheidskenmerken** ▪ Aandachtscontrole ▪ Bewustzijn ▪ Computerkennis/-vaardigheden ▪ Zelfbeheersing	**Intrinsieke en persoonlijkheidskenmerken** -
Routine activiteiten -	**Routine activiteiten** -	**Routine activiteiten** ▪ Internetgebruik

1/2

↩ Terug naar de overzichtspagina van dit hoofdstuk

1.4.3 RISICOFACTOREN ONLINE CRIMINALITEIT

SLACHTOFFERSCHAP | Risicofactoren phishing | 2/2

RISICOFACTOREN | SLACHTOFFERSCHAP | PHISHING		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Macrofactoren -	**Macrofactoren** -	**Macrofactoren** ▪ Bedrijfscultuur
Overige factoren -	**Overige factoren** -	**Overige factoren** ▪ Prevalentie effect

INTERVENTIES EN TRAININGEN | SLACHTOFFERSCHAP | PHISHING		
Opkomend/aanbeveling	**Niet opkomend/geen aanbeveling**	**Onduidelijk**
Interventies ▪ Technologische tekorten	**Interventies** ▪ Mobiele applicaties ▪ User interface ▪ Waarschuwingsberichten	**Interventies** -
Trainingen ▪ Belonen en straffen ▪ Klassikale training	**Trainingen** ▪ Algemeen ▪ Feedback ▪ Games ▪ Gepersonaliseerde training ▪ Herhaling ▪ Ingebedde training	**Trainingen** -

2/2

↩ Terug naar de overzichtspagina van dit hoofdstuk

1.4.4 RISICOFACTOREN ONLINE CRIMINALITEIT

SLACHTOFFERS | Fear of cybercrime

SLACHTOFFERSCHAP | Risicofactoren fear of cybercrime

RISICOFACTOREN | SLACHTOFFERSCHAP | FEAR OF CYBERCRIME		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Demografische kenmerken ▪ Geslacht (vrouw)	**Demografische kenmerken** -	**Demografische kenmerken** ▪ Leeftijd ▪ Etniciteit ▪ Inkomen ▪ Opleiding ▪ Werk
Intrinsieke en persoonlijkheidskenmerken ▪ Waargenomen risico	**Intrinsieke en persoonlijkheidskenmerken** -	**Intrinsieke en persoonlijkheidskenmerken** -
Mentaal ▪ Angst	**Mentaal** -	**Mentaal** -
Sociale relaties ▪ Relatiestatus	**Sociale relaties** -	**Sociale relaties** -
Routine activiteiten -	**Routine activiteiten** -	**Routine activiteiten** ▪ Internetgebruik ▪ Online activiteiten
Criminaliteit ▪ Eerder slachtofferschap ▪ Kenmerken dader	**Criminaliteit** -	**Criminaliteit** ▪ Type criminaliteit

↩ Terug naar de overzichtspagina van dit hoofdstuk

PARAGRAAF 1.5

Bevindingen: risicofactoren slachtofferschap online criminaliteit

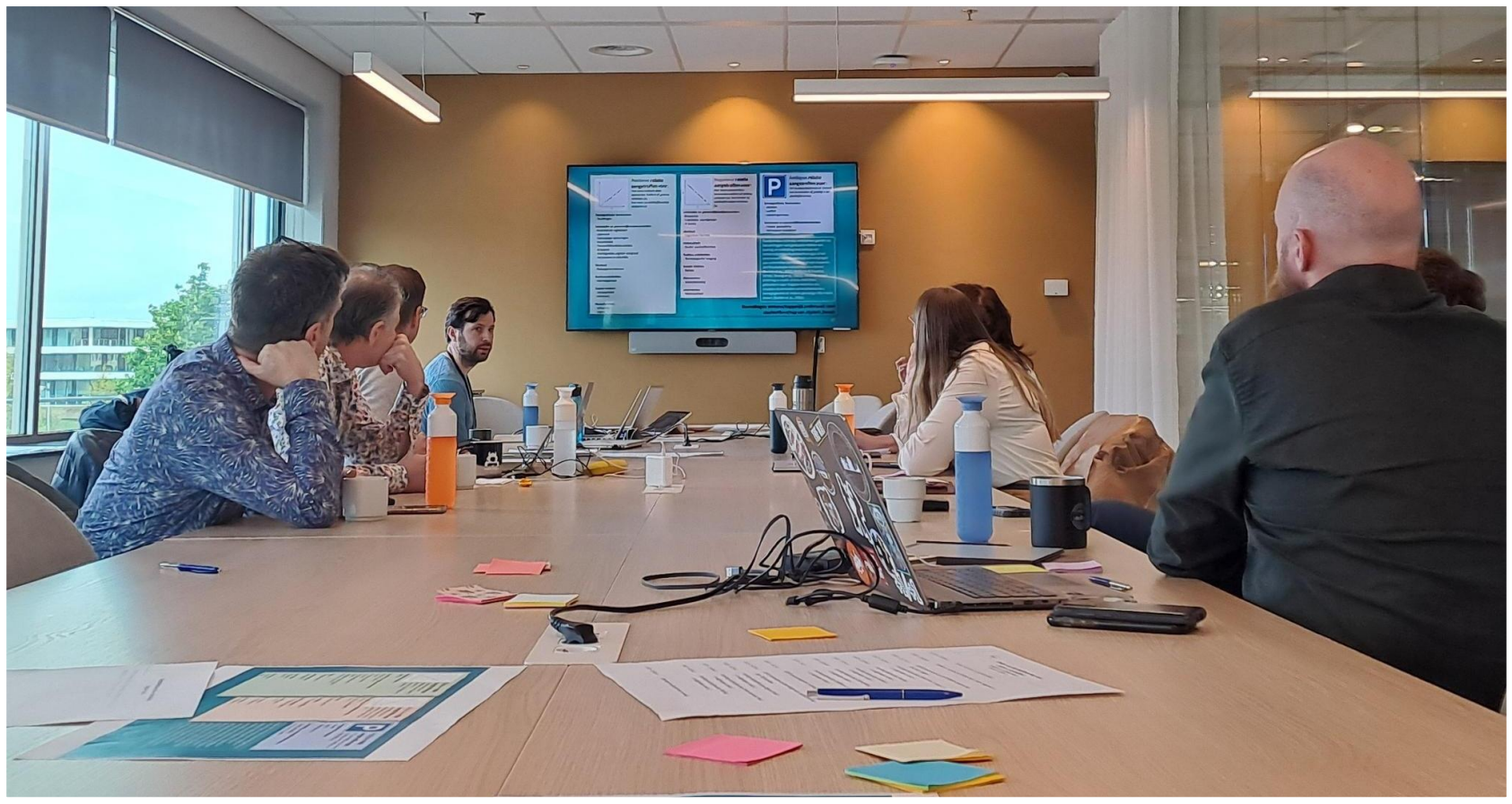
Totaaloverzicht

1.5 RISICOFACTOREN ONLINE CRIMINALITEIT

SLACHTOFFERSCHAP | Risicofactoren totaaloverzicht

RISICOFACTOREN | SLACHTOFFERSCHAP | TOTAALOVERZICHT		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Demografische kenmerken ▪ Geslacht (vrouw)	**Demografische kenmerken** -	**Demografische kenmerken** ▪ Leeftijd ▪ Opleidingsniveau ▪ Etniciteit ▪ Inkomen
Intrinsieke en persoonlijkheidskenmerken ▪ Gevoelig voor autoriteit	**Intrinsieke en persoonlijkheidskenmerken** ▪ Zelfbeheersing ▪ Bewustzijn ▪ IT-kennis en computer-vaardigheden	**Intrinsieke en persoonlijkheidskenmerken** -

↩ Terug naar de overzichtspagina van dit hoofdstuk



Afbeelding: eigen bezit, gemaakt tijdens kennissessie met praktijkpartners op 24 april 2024

HOOFDSTUK 2

Resultaten focusgroep: Inzichten uit de praktijk over dader- en slachtofferschap van online criminaliteit

Elmira Land BA & dr. Remco Spithoven

Lectoraat Online Weerbaarheid, Hogeschool Saxion

OPBOUW HOOFDSTUK

HOOFDSTUK 2: RESULTATEN FOCUSGROEP

Opgedane inzichten uit de praktijk met betrekking tot dader- en slachtofferschap van online criminaliteit

2.1: Toelichting vooraf

2.2: Bevindingen daderschap online criminaliteit – inzichten algemeen

2.3: Bevindingen slachtofferschap online criminaliteit – inzichten algemeen

BIJLAGE 1: INZICHTEN UIT DE PRAKTIJK

Bijlage 1.1: Daderschap

- Bijlage 1.1.1: Online criminaliteit, overkoepelend
- Bijlage 1.1.2: Cybercrime in enge zin
- Bijlage 1.1.3: Cyberstalking
- Bijlage 1.1.4: Malware
- Bijlage 1.1.5: Strafbare vormen van sexting
- Bijlage 1.1.6: Hacking
- Bijlage 1.1.7: Online fraude

Bijlage 1.2: Slachtofferschap

- Bijlage 1.2.1: Online criminaliteit, overkoepelend
- Bijlage 1.2.2: Online fraude
- Bijlage 1.2.3: Datingfraude
- Bijlage 1.2.4: Phishing

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

↩ Terug naar de inhoudsopgave

2.1 TOELICHTING VOORAF

In dit hoofdstuk worden de bevindingen besproken die uit focusgroep met ervaren professionals die op 24 april 2024 plaatsvond in Utrecht. Tijdens deze focusgroep werden allereerst de resultaten van de systematische, narratieve review naar risicofactoren voor slachtoffer- en daderschap van online criminaliteit uit het vorige hoofdstuk gepresenteerd. Praktijkpartners hebben hier feedback op gegeven op basis van hun praktijkkennis en –ervaring. In dit hoofdstuk wordt de opbrengst van deze focusgroep beschreven in tabelvorm, gesorteerd op inzichten voor slachtoffer- en daderschap.

Ook hebben Peter Hagenaars en Remco Spithoven de resultaten uit de systematische, narratieve review gepresenteerd op de de Global Anti Scam Summit op 25 juni 2024 in Brussel. Op dit internationale congres waren professionals in de aanpak van online fraude bijeen.

Uit deze sessie zijn niet zozeer concrete aanvullingen gekomen maar werden de resultaten vooral herkend en gewaardeerd. De aanvullingen die werden gegeven, kwamen overeen met de aanvullingen van de Nederlandse professionals.

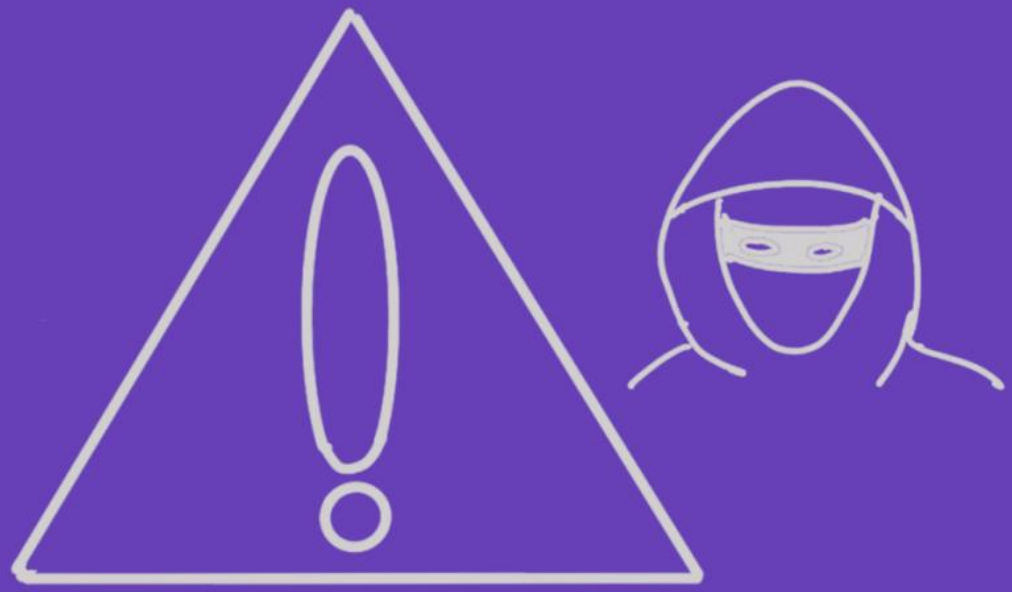
Beide praktijksessies hebben waardevolle inzichten opgeleverd voor het vervolg van dit onderzoek en worden daarom ook in dit verslag meegenomen.

In dit hoofdstuk worden de samengevatte praktijkinzichten weergegeven voor slachtoffer- en daderschap in het algemeen. In bijlage 1 van dit document staan de inzichten per delictstype (zie deze bijlage of de dia hiervoor voor een overzicht van deze delictstypen).

Praktijksessie 24 april 2024

Global Anti Scam Summit
25 juni 2024

↩ Terug naar de overzichtspagina van dit hoofdstuk



PARAGRAAF 2.2

Inzichten uit de praktijk: risicofactoren daderschap online criminaliteit

Totaaloverzicht

2.2 BEVINDINGEN UIT DE PRAKTIJK

DADERSCHAP | Online criminaliteit, overkoepelend

INZICHTEN PRAKTIJKSESSIE | DADERSCHAP | ONLINE CRIMINALITEIT, OVERKOEPELEND			
Wat wordt herkend en wat mist er nog?	**Wat betekent dit in het voorkomen van daderschap?**	**Beleidsstukken, analyses of andere bronnen?**	**Good practices uit binnen- en buitenland**
Er mist nog: ▪ Meer informatie over de invloed van **geslacht** en **leeftijd**; ▪ Onderscheid tussen **cybercrime** en **gedigitaliseerde criminaliteit**; ▪ Meer informatie over relatie qua **criminele carrière** en qua '**crimineel werkveld**' tussen online criminaliteit, vormen van ondermijnende/georganiseerde criminaliteit; ▪ Nog meer focus op **daderschap** van **veel voorkomende online criminaliteit**, want dat is nu heel actueel!	▪ Via politieonderzoek naar daders kan je de **school identificeren** en **weerbaarheidsinstructie** inzetten; ▪ Gericht onderzoek doen naar de plaatsen op internet waar **'social learning**' plaatsvindt en dan offline halen; ▪ **Privaatrechtelijk aansprakelijk stellen**, **stopgesprek** ed.; ▪ Zie aanpak **COPS** (Cyber Offender Prevention Squad), voor deze doelgroep; ▪ Dit is moeilijk zonder onderscheid tussen **'high tech**' vs **'low tech**'; ▪ **Social media** (bv Snapchat ads) inzetten om mensen met deze kenmerken te targetten.	▪ Geen, alle onderzoek is 'in statu nascendi'; ▪ Het **fenomeenbeeld analyse 2024** ("Online Fraude in Beeld"); ▪ De inzet van **Google ads**.	▪ **COPS**: Cyber Offender Prevention Squad van de Nederlandse politie; ▪ Geen, maar wel actief op zoek bilateraal naar EU-partners.

↩ Terug naar de overzichtspagina van dit hoofdstuk

PARAGRAAF 2.3

Inzichten uit de praktijk: risicofactoren slachtofferschap online criminaliteit

Totaaloverzicht

2.3 BEVINDINGEN UIT DE PRAKTIJK

SLACHTOFFERSCHAP | Online criminaliteit, overkoepelend | 1/2

INZICHTEN PRAKTIJKSESSIE | SLACHTOFFERSCHAP | ONLINE CRIMINALITEIT, OVERKOEPELEND

Wat wordt herkend en wat mist er nog?

Wat werd herkend:
- De **gevoeligheid voor autoriteit;**
- Algemeen.

Vragen rezen over:
- Het **geslacht**; waarom zijn vrouwen meer slachtoffer? Input ging over het feit dat dit misschien wel voor romance fraud zou gelden, maar niet voor bijvoorbeeld aan- en verkoopfraude;
- **Geldezels** binnen het geschetste beeld. Valt dit onder dader- of slachtofferschap?;
- Zijn slachtoffers “extra” **kapitaal krachtig**?

Wat nog miste:
- Meer nuance wat betreft het **geslacht** van de slachtoffers;
- Meer nuance wat betreft de **leeftijd** van de slachtoffers (“verschilt ook sterk per delict bijvoorbeeld sextortion (jong) en bankhelpdeskfraude (oud)”);
- Meer informatie over **cyberschaamte**;
- De invloed van een **“brave" omgeving**, zoals een dorpje;
- **Ambiguïteit**: er is een duidelijk onderscheid te maken in leeftijd/geslacht tussen verschillende vormen van online fraude;
- **IT skills** zouden ook naar **ambigu** moeten;
- Meer **algemene campagnes** die werken met "Zonde van het geld“.

1/2

↩ Terug naar de overzichtspagina van dit hoofdstuk

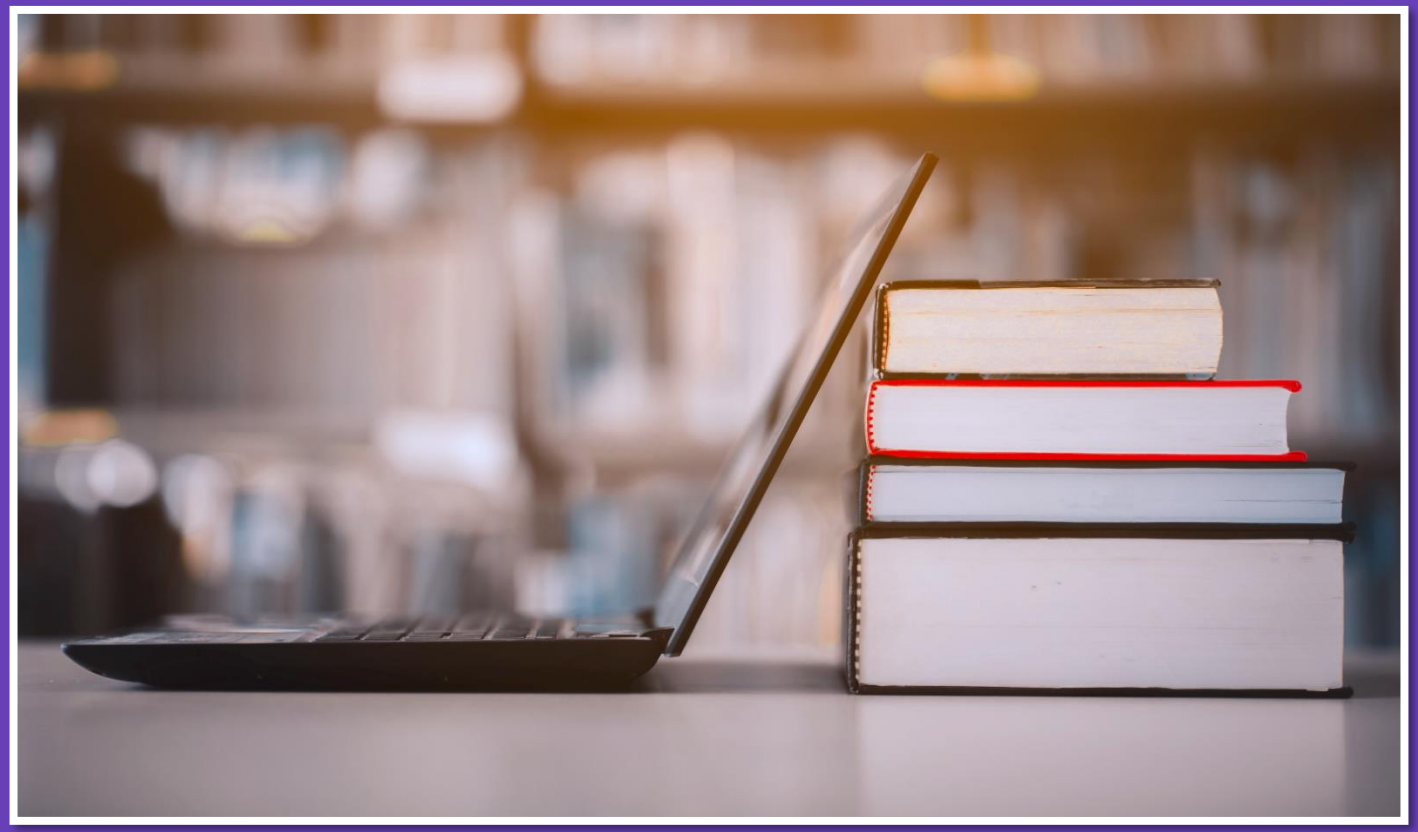
2.3 BEVINDINGEN UIT DE PRAKTIJK

SLACHTOFFERSCHAP | Online criminaliteit, overkoepelend | 2/2

INZICHTEN PRAKTIJKSESSIE | SLACHTOFFERSCHAP | ONLINE CRIMINALITEIT, OVERKOEPELEND		
Wat betekent dit in het voorkomen van daderschap?	**Beleidsstukken, analyses of andere bronnen?**	**Good practices uit binnen- en buitenland**
▪ [Er is(?)] **lage computerkennis**; ▪ Ander profiel bij de bank, daarmee **eerdere detectie**; ▪ Bij bankhelpdeskfraude heeft het slachtoffer na ophangen direct door dat het niet klopt, tijdens gesprek ook al onbehagen; ▪ De **Modus Operandi** verstoren; ▪ **Gelegenheidsstructuren** verstoren; ▪ **Cyberschaamte** doorbreken; ▪ **Meldingsbereidheid** vergroten; ▪ Focus op **preventie én nazorg**; ▪ **Ervaringsverhalen** delen; ▪ Koppeling tussen **hulp, nazorg en preventie** z.s.m. bij melding (of waar dan ook) om herhaald slachtofferschap te voorkomen; ▪ Het **identificeren van plaatsen** voor b.v. datingfraude en daar **detectie** en **preventiemaatregelen** op zetten; ▪ Het **nabootsen** van **slachtofferschap**; ▪ Voorkomen van delict (**verstoren**) heeft meer impact dan voorkomen door **voorlichting**; ▪ Een **gespecialiseerd team** inrichten voor online slachtofferpreventie.	▪ Onderzoek **cyberschaamte** politie Rotterdam, cyber en communicatie – 2x genoemd; ▪ Onderzoek **meldingsbereidheid** van **slachtoffers** van **Ransomware** in de haven van Rotterdam; ▪ Microdata van het **CBS**; ▪ Onderzoeken van **GASA**; ▪ Onderzoek van UT over **Fraudevictimisatie**; ▪ **Fenomeenbeeld** '24 Politie (“Online Fraude in Beeld”); ▪ Onderzoek van Jildau Borwell; ▪ Check **cyberbeelden** politie voor delicten vs. leeftijd; ▪ Onderzoek van de **consumentenbond** uit ‘23.	▪ **Scam survivors** in het Verenigd Koninkrijk; ▪ **WhatsNep** in Nederland; ▪ **Echt of nep?** In Nederland - Rotterdam (Interactieve film), werd 2x genoemd.

2/2

↩ Terug naar de overzichtspagina van dit hoofdstuk



Afbeelding: Stockfoto

HOOFDSTUK 3

Resultaten scoping review:
Daderschap van online criminaliteit in de wetenschappelijke literatuur tussen 2021 - 2024

Thijs van Beek MSc. & dr. Remco Spithoven

Lectoraat Online Weerbaarheid, Hogeschool Saxion.

OPBOUW HOOFDSTUK

HOOFDSTUK 3: RESULTATEN SCOPING REVIEW

Daderschap online criminaliteit in wetenschappelijke literatuur

3.1: Toelichting vooraf

3.2: Samenvatting bevindingen daderschap online criminaliteit – per delictstype

- 3.2.1: Online criminaliteit, overkoepelend
- 3.2.2: Cybercrime in enge zin
- 3.2.3: Phishing/vishing
- 3.2.4: Online fraude
- 3.2.5: Geldezels
- 3.2.6: Social engineering
- 3.2.7: Bitcoin gerelateerde online criminaliteit

3.3: Bevindingen daderschap online criminaliteit – totaaloverzicht

BIJLAGE 2: INZICHTEN UIT DE WETENSCHAP – SCOPING REVIEW

Bijlage 2.1: Hacking	Bijlage 2.9: E-commerce fraude
Bijlage 2.2: Malware	Bijlage 2.10: Concession-Abuse-as-a-Servive (CAaaS)-fraude
Bijlage 2.3: Online fraude	Bijlage 2.11: Online werkgelegenheids-fraude
Bijlage 2.4: Phishing	Bijlage 2.12: Online werknemersfraude
Bijlage 2.5: Vishing	Bijlage 2.13: Online bankpasfraude
Bijlage 2.6: Datingfraude	Bijlage 2.14: Social engineering
Bijlage 2.7: Pig-butchering scam	Bijlage 2.15: Geldezels
Bijlage 2.8: Advance fee fraud	Bijlage 2.16: Bitcoin-gerelateerde criminaliteit
	Bijlage 2.17: Overig

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

↩ Terug naar de inhoudsopgave

3.1 TOELICHTING VOORAF

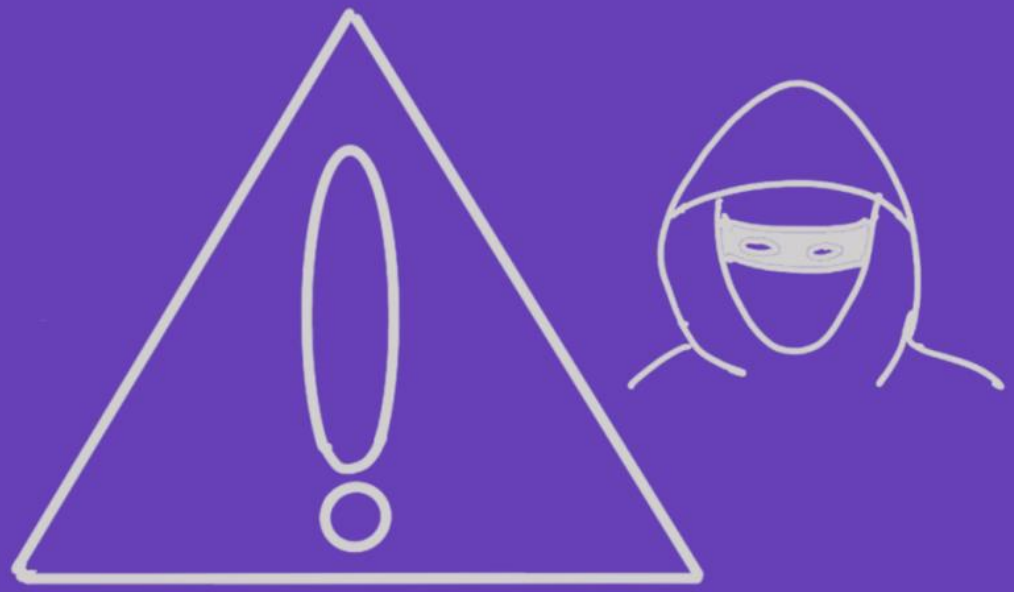
In dit hoofdstuk worden de resultaten van de scoping review op hoofdlijnen besproken. Het omvangrijke deelrapport is via de link te downloaden als pdf-bestand. Voor deze scoping review zijn losse, wetenschappelijke artikelen geraadpleegd om informatie te verzamelen over risicofactoren voor *dader*schap van online criminaliteit, en de daarmee verbonden interventies.

Via een search query **tot en met 4 december 2024** is er gezocht in zes online databases naar losse, wetenschappelijke publicaties die tussen 2021 en 2024 zijn gepubliceerd, om zo een overzicht te krijgen van de meest recente bevindingen. Dit resulteerde in 52 relevante studies van de bestaande literatuur. De inzichten hieruit worden in dit hoofdstuk besproken als geheel van inzichten op het gebied van daderschap van online criminaliteit. In bijlage 2 worden de resultaten per delictstype weergegeven.

Om de resultaten uit deze scoping review overzichtelijk weer te kunnen geven, is er wederom met een aantal kleuren gewerkt. Dit is zowel in dit hoofdstuk, als in bijlage 2 aan de orde. Omwille van de omvang van de tabellen op de hierna volgende dia's, wordt de legenda voor de gebruikte kleuren hieronder alvast weergegeven.

Positieve relatie	Hoe meer iemand dit kenmerk heeft of dit gedrag vertoont, hoe groter de kans dat hij of zij dader of slachtoffer wordt.
Negatieve relatie	Hoe meer iemand dit kenmerk heeft of dit gedrag vertoont, hoe kleiner de kans dat hij of zij dader of slachtoffer wordt.
Ambigue relatie	het is onduidelijk wat de invloed van dit kenmerk of dit gedrag is op dader- of slachtofferschap.

↩ Terug naar de overzichtspagina van dit hoofdstuk



PARAGRAAF 3.2

Samenvatting bevindingen: risicofactoren daderschap online criminaliteit

Overzicht per delictstype

3.2.1 BEVINDINGEN WETENSCHAPPELIJKE LITERATUUR

DADERSCHAP | Overzicht o.b.v. losse publicaties 2021-2024 | Online criminaliteit, overkoepelend

SAMENVATTING INZICHTEN WETENSCHAPPELIJKE LITERATUUR | DADERSCHAP | ONLINE CRIMINALITEIT, OVERKOEPELEND				
Positieve relatie	▪ Afpersing ▪ AI-technologie ▪ Anonimiteit (t) ▪ Armoede ▪ Avengers ▪ Bewustzijn (i) ▪ Cognitieve bias ▪ Cognitieve gedragstheorie ▪ Context en landen (o) ▪ Corporate crimes (t) ▪ Cryptocurrency (t) ▪ Cultuur ▪ Cyberoorlog & normalisatie (o) ▪ Daderperspectief (o) ▪ DarkNet (t) ▪ Dehumanisering ▪ Detectie (i) ▪ Digitaal bewijs (t) ▪ Digitale ruimte (ethische filter)	▪ Disrespect ▪ Economische rechtvaardiging ▪ Ethisch gedrag (i) ▪ Evaluatie (o) ▪ Extravagante levensstijl (t) ▪ Faciliterende factoren (o) ▪ Financieel gewin ▪ Financiële problemen ▪ Frequentie (t) ▪ Gebruik van persoonsgegevens ▪ Gemeenschap ▪ Geslacht (man) ▪ Groeiende dreiging (t) ▪ Groepsdruk ▪ Hogere loyaliteiten ▪ Innovatieve methodes (i) ▪ Intimidatie ▪ IT-kennis ▪ Kant-en-klare tools (t)	▪ Koloniaal verleden ▪ Maatschappelijke eisen ▪ Meervoudige dader ▪ Migratie ▪ Migratiestatus ▪ Monitoren (i) ▪ Ondersteuning slachtoffer (i) ▪ Ongelijkheid ▪ Online platforms ▪ Ontkennen van schade ▪ Ontkennen van slachtofferschap ▪ Ontkennen van verantwoordelijk-heid ▪ Peers ▪ Psychoanalytische theorie ▪ Risico van AI (t) ▪ Risicobeoordeling (i) ▪ Risicogedrag ▪ Samenwerking (i)	▪ Seksuele uitbuiting ▪ Sociaal leertheorie (o) ▪ Sociaalgerichte intervent. (i) ▪ Socio-economische interventie (i) ▪ Space Transition theorie ▪ Steekproef (o) ▪ Stress ▪ Traditioneel en online sociaal leren ▪ Verdienmodel (i) ▪ Veroordelen van de veroordelaars ▪ Wetgeving (i) ▪ Wetshandhaving ▪ Wisselende MO ▪ Wraak ▪ Zelfbeschermings-maatregelen (i)
Negatieve relatie	▪ Empathie ▪ Morele ontwikkeling	▪ Opleidingsniveau ▪ Ouderschap	▪ Religieuze overtuigingen ▪ Sociale banden	▪ Zelfcontrole
Ambigue relatie	▪ Altruïsme ▪ Leeftijd			

ⓘ - (t) = trends, (o) = toekomstig onderzoek, (i) = interventies/trainingen

↩ Terug naar de overzichtspagina van dit hoofdstuk

3.2.2 BEVINDINGEN WETENSCHAPPELIJKE LITERATUUR

DADERSCHAP | Overzicht o.b.v. losse publicaties 2021-2024 | Cybercrime in enge zin

SAMENVATTING INZICHTEN WETENSCHAPPELIJKE LITERATUUR | DADERSCHAP | CYBERCRIME IN ENGE ZIN				
Positieve relatie	▪ Bewustzijn schade (i) ▪ Blokkeren van toegang ▪ Chatrooms en sociale media (o) ▪ Frequentie (t) ▪ Game-items ▪ Gebruikte kanalen ▪ Geslacht en leeftijd ▪ Internetgebruikers	▪ Koopbaarheid van persoonsgegevens ▪ Monitoren (i) ▪ Multilevel model (o) ▪ Neutralisatie-technieken (i) (algemeen) ▪ Ontkennen van slachtofferschap	▪ Peers ▪ Persoonlijke informatie ▪ Plezier en impulsiviteit ▪ Rechtvaardigingsclaim ▪ Social engineering ▪ Steekproef (o) ▪ Strafblad en recidive ▪ Veroordelaars veroordelen	▪ Verspreiding van schuld ▪ Verspreiding via download of bijlages in e-mails ▪ Woede
Negatieve relatie	▪ Persoonlijke rechtvaardiging	▪ Relatie tot het slachtoffer (t) ▪ Welvaart		
Ambigue relatie	▪ Afschrikking (i) ▪ Chatrooms ▪ Ontkennen van schade	▪ Persoonlijke rechtvaardiging	▪ Rechtvaardiging o.b.v. noodzaak	▪ Verantwoordelijkheid ontkennen

ⓘ - (t) = trends, (o) = toekomstig onderzoek, (i) = interventies/trainingen

↩ Terug naar de overzichtspagina van dit hoofdstuk

3.2.3 BEVINDINGEN WETENSCHAPPELIJKE LITERATUUR

DADERSCHAP | Overzicht o.b.v. losse publicaties 2021-2024 | Phishing/vishing

SAMENVATTING INZICHTEN WETENSCHAPPELIJKE LITERATUUR | DADERSCHAP | PHISHING/VISHING				
Positieve relatie	▪ Algemene termen in e-mails ▪ Autoriteit (2x) ▪ Behulpzaamheid ▪ Decoy-pagina's ▪ Dreiging ▪ Phishingkits ▪ Sociale context ▪ Disproportioneel aandeel (t)	▪ Frequentie (t) ▪ Motivatie oplichter (o) ▪ Sociale contexten ▪ Sociale manipulatie (o) ▪ Vergelijkend onderzoek (o) ▪ Adequaat handelen (i) ▪ Bewustwording (i) ▪ Detectiemethoden (i) ▪ Monitoren (i)	▪ Phishingkits repository (i) ▪ Wetshandhaving (i) ▪ Financieel gewin ▪ Interactie ▪ Rekrutering ▪ Volp-technologie ▪ Onder druk zetten	▪ Bewustwording (i) ▪ Misdaad-scripts (o) (i) ▪ Samenwerking (i)
Negatieve relatie	▪ Levensduur phishing-aanval			
Ambigue relatie	-			

ⓘ - (t) = trends, (o) = toekomstig onderzoek, (i) = interventies/trainingen

↩ Terug naar de overzichtspagina van dit hoofdstuk

3.2.4 BEVINDINGEN WETENSCHAPPELIJKE LITERATUUR

DADERSCHAP | Overzicht o.b.v. losse publicaties 2021-2024 | Online fraude

SAMENVATTING INZICHTEN WETENSCHAPPELIJKE LITERATUUR | DADERSCHAP | ONLINE FRAUDE					
Positieve relatie	▪ Altercasting ▪ Anonimiteit ▪ Bedrijfsinterventies (i) ▪ Betaalbaarheid ▪ Betrokkenheid bij niet-oplichters-praktijken ▪ Crimineel gedrag en mechanismen ▪ Criminele netwerken en juridische ontwijking ▪ Demografische onderzoeksfocus (o)	▪ Digitale en technologische technieken ▪ Ecologische en externe validiteit (o) ▪ Evaluatie en toekomstgerichte maatregelen (i) ▪ Familiaire invloed ▪ Financieel gewin ▪ Focus op niet-technologisch beroep ▪ Frequentie (t) ▪ Genderrollen in criminaliteit	▪ Groepsinteractie ▪ Internetgebruik ▪ Menselijk gedrag ▪ Mentorschap ▪ Modus operandi ▪ Monitoring, detectie en regulering (i) ▪ Neutralisatietechnieken ▪ Normalisatie en rechtvaardiging ▪ Ondersteuning en herstel (i) ▪ Ondeugd	▪ Ongebruikelijk gedrag ▪ Onvoldoende toezicht ▪ Patriarchale normen ▪ Preventie en bewustwording (i) ▪ Preventie en impact (i) ▪ Psychologische en sociale manipulatie ▪ Psychologische onderzoeksfocus (o) ▪ Repressie, wetgeving en handhaving (i)	▪ Salaristarieven manipuleren ▪ Sociaal-economische en politieke omstandigheden ▪ Social engineering ▪ Sociale banden ▪ Verspreiding van criminele kennis en vaardigheden ▪ Waarschuwings-berichten (i) ▪ Witwassen en geldstromen
Negatieve relatie	▪ Directe interactie ▪ Leeftijd	▪ Nepaccounts identificeren (t)	▪ SES en opleidingsniveau	▪ Strafblad ▪ Welvaart	
Ambigue relatie	▪ Geslacht en werkpositie ▪ Leeftijd				

ⓘ - (t) = trends, (o) = toekomstig onderzoek, (i) = interventies/trainingen

↩ Terug naar de overzichtspagina van dit hoofdstuk

3.2.5 BEVINDINGEN WETENSCHAPPELIJKE LITERATUUR

DADERSCHAP | Overzicht o.b.v. losse publicaties 2021-2024 | Geldezels

SAMENVATTING INZICHTEN WETENSCHAPPELIJKE LITERATUUR | DADERSCHAP | GELDEZELS		
Positieve relatie	▪ Accounts blokkeren (i) ▪ Anonimiteit verminderen (i) ▪ Bewustwording (i) ▪ Misbruik financiële problemen ▪ Gesloten netwerken ▪ Instagram ▪ Monitoren en waarschuwingen (i)	▪ Neutralisatie- en normalisatietechnieken ▪ Peer pressure en subculturele normen (i) ▪ Presenteren als reguliere bedrijven ▪ Privé-chats ▪ Regionale gerichtheid ▪ Subcultuur (t) ▪ Voorlichting (i)
Negatieve relatie	-	
Ambigue relatie	-	

ⓘ - (t) = trends, (o) = toekomstig onderzoek, (i) = interventies/trainingen

↩ Terug naar de overzichtspagina van dit hoofdstuk

3.2.6 BEVINDINGEN WETENSCHAPPELIJKE LITERATUUR

DADERSCHAP | Overzicht o.b.v. losse publicaties 2021-2024 | Social engineering

SAMENVATTING INZICHTEN WETENSCHAPPELIJKE LITERATUUR | DADERSCHAP | SOCIAL ENGINEERING		
Positieve relatie	▪ Authenticiteit ▪ Autoriteit ▪ Beloning en behulpzaam zijn ▪ Demografische factoren (o) ▪ Gedrag afstemmen ▪ Modus operandi en detectie-mechanismen (o) ▪ Motivatie (o) ▪ Normaal overkomen	▪ Overtuigend profiel ▪ Psychologische en sociale mechanismen van slachtoffers (o) ▪ Realistisch scenario schetsen ▪ Snel en eenvoudig ▪ Sociale norm ▪ Timing ▪ Urgentie en druk
Negatieve relatie	-	
Ambigue relatie	-	

ⓘ - (t) = trends, (o) = toekomstig onderzoek, (i) = interventies/trainingen

↩ Terug naar de overzichtspagina van dit hoofdstuk

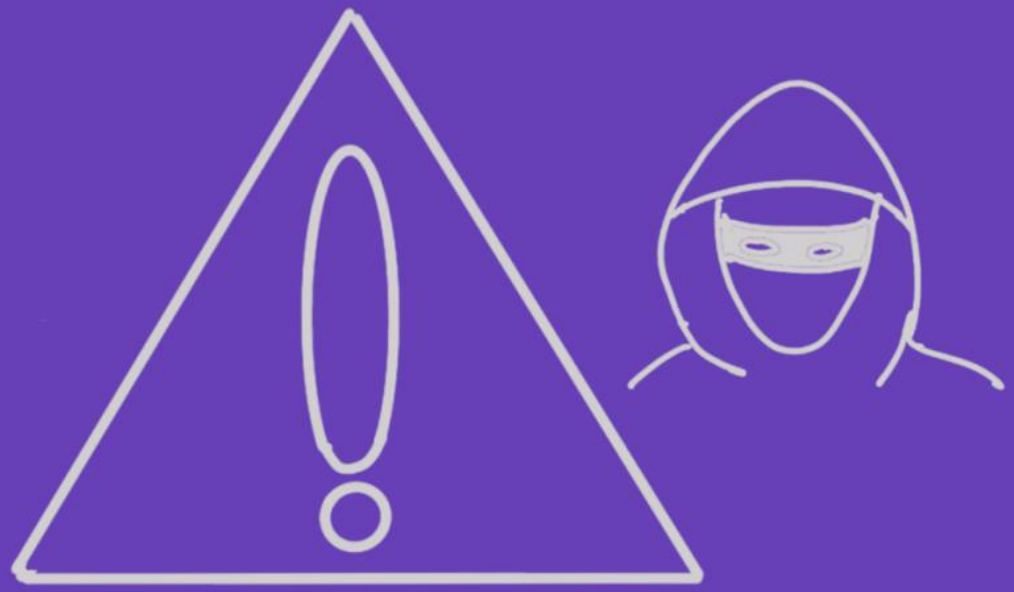
3.2.7 BEVINDINGEN WETENSCHAPPELIJKE LITERATUUR

DADERSCHAP | Overzicht o.b.v. losse publicaties 2021-2024 | Bitcoin gerelateerde online criminaliteit

SAMENVATTING INZICHTEN WETENSCHAPPELIJKE LITERATUUR | DADERSCHAP | BITCOIN GERELATEERDE ONLINE CRIMINALITEIT	
Positieve relatie	▪ Bewustwording (i) ▪ Concentratie criminaliteit (t) ▪ Detectie (i)
Negatieve relatie	-
Ambigue relatie	-

ⓘ - (t) = trends, (o) = toekomstig onderzoek, (i) = interventies/trainingen

↩ Terug naar de overzichtspagina van dit hoofdstuk



PARAGRAAF 3.3

Samenvatting bevindingen: risicofactoren daderschap online criminaliteit

Totaaloverzicht

3.3 BEVINDINGEN WETENSCHAPPELIJKE LITERATUUR

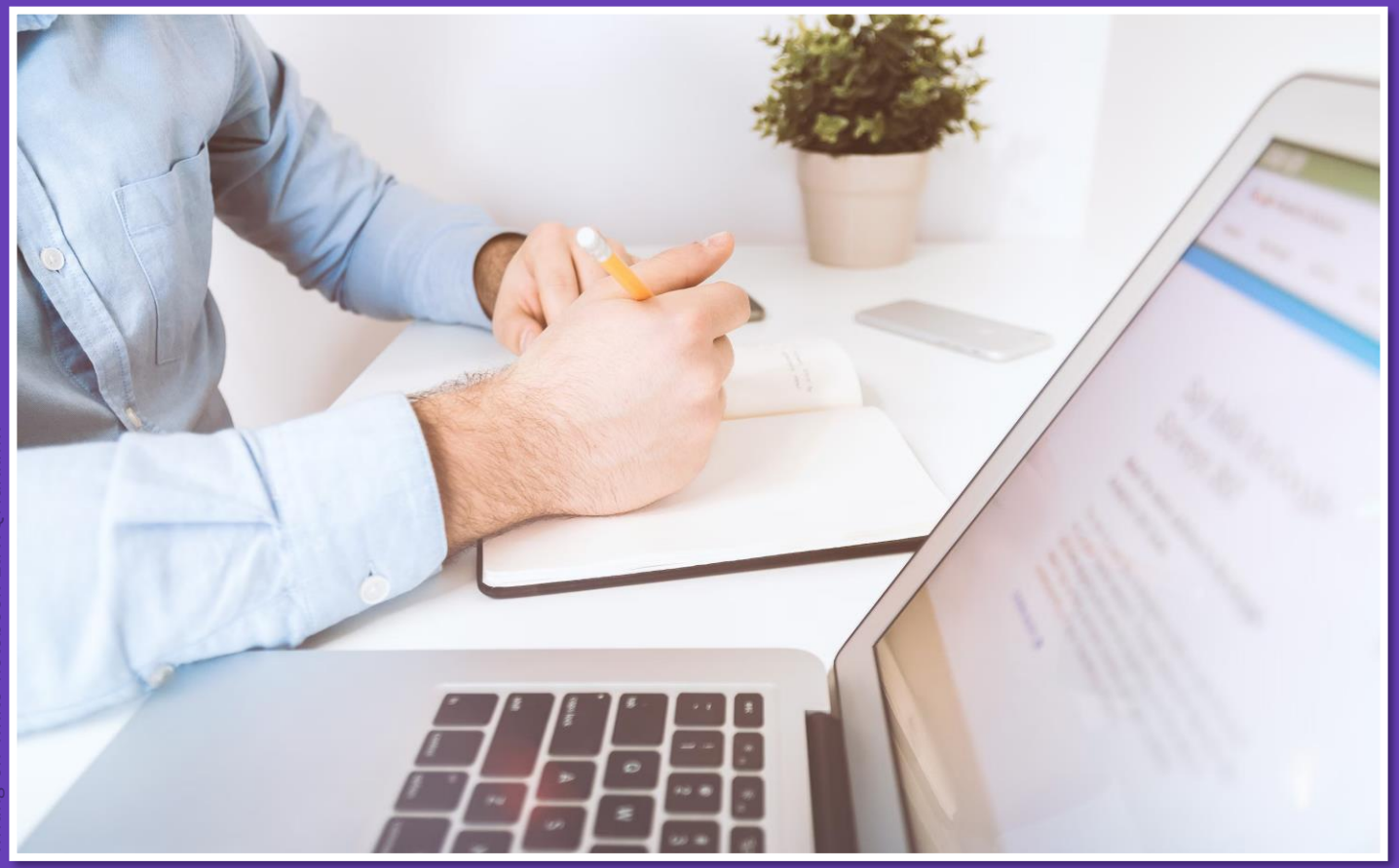
DADERSCHAP | Totaaloverzicht o.b.v. losse publicaties 2021-2024

DADERS | Totaal-overzicht

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macrofactoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/dader)
Geslacht (man)	IT-kennis		Gemeenschap	Armoede	Dehumanisering	AI-technologie	+ Anonimiteit	+ Context en landen	+ Bewustzijn
Migratiestatus	Morele ontwikkeling		Groepsdruk	Cultuur	Digitale ruimte (ethische filter)	Gebruik van persoonsgegevens	+ Corporate crimes	+ Cyberoorlog en normalisatie	+ Detectie
Opleidingsniveau	Cognitieve bias		Intimidatie	Maatschappelijke eisen	Economische rechtvaardiging	Netwerk	+ Cruptocurrency	+ Dader-perspectief	+ Innovatieve methodes
Leeftijd	Cognitieve gedragstheorie		Peers	Migratie	Hogere loyaliteiten	Online platforms	+ Darkweb	+ Evaluatie	+ Monitoren
	Psycho-analytische theorie		Traditioneel en online sociaal leren	Ongelijkheid	Koloniaal verleden	Wisselende MO	+ Digitaal bewijs	+ Faciliterende factoren	+ Ondersteuning slachtoffer
	Risicogedrag		Ouderschap	Wetgeving en wetshandhaving	Ontkennen van schade		+ Extravagante levensstijl	+ Method een data-analyse	+ Risicobeoordeling
	Space transition theorie		Sociale banden	Religieuze overtuigingen	Ontkennen van slachtofferschap		+ Frequentie	+ Sociale leertheorie	+ Samenwerking
	Stress				Ontkennen van verantwoordelijkheid		+ Groeiende dreiging	+ Steekproef	+ Wetgeving
	Empathie				Veroordelen van de veroordelaars		+ Kant-en-klare tools		+ Zelfbeschermings-maatregelen
	Zelfcontrole				Afpersing		+ Risico van AI		+ Cognitive bias
	Meervoudige dader				Avengers				+ Ethisch gedrag
					Disrespect				+ Sociaalgerichte interventies
					Financieel gewin				+ Socio-economische interventie
					Financiële problemen				+ Verdienmodel
					Hebzucht				
					Seksuele uitbuiting				
					Wraak				
					Altruïsme				

Legenda

↩ Terug naar de overzichtspagina van dit hoofdstuk



Afbeelding: Unsplash. (2017, 8 maart). https://unsplash.com/photos/person-writing-on-white-notebook-LtNvQHdkkmw

HOOFDSTUK 4

Resultaten praktijkgerichte literatuur: Interventies en initiatieven met betrekking tot aanpakken van dader- en slachtofferschap online criminaliteit

Elmira Land BA & dr. Remco Spithoven

Lectoraat Online Weerbaarheid, Hogeschool Saxion.

OPBOUW HOOFDSTUK

HOOFDSTUK 4: RESULTATEN GRIJZE LITERATUUR

Interventies en initiatieven met betrekking tot dader- en slachtofferschap online criminaliteit

4.1: Toelichting vooraf

4.2: Bevindingen daderschap online criminaliteit – totaaloverzicht 35 interventies

4.3: Bevindingen slachtofferschap online criminaliteit – totaaloverzicht 86 interventies

BIJLAGE 3: INZICHTEN UIT DE PRAKTIJKGERICHTE LITERATUUR

Bijlage 3.1: Daderschap

- Bijlage 3.1.1: Algemene weerbaarheid
- Bijlage 3.1.2: Hacking + mal-/ransomware
- Bijlage 3.1.3: Online fraude
- Bijlage 3.1.4: Online geweld/cyberpesten
- Bijlage 3.1.5: Phishing
- Bijlage 3.1.6: Sexting/sextortion/grooming
- Bijlage 3.1.7: Overig

Bijlage 3.2: Slachtofferschap

- Bijlage 3.2.1: Algemene weerbaarheid
- Bijlage 3.2.2: Hacking + mal-/ransomware
- Bijlage 3.2.3: Online fraude
- Bijlage 3.2.4: Online geweld/cyberpesten
- Bijlage 3.2.5: Phishing
- Bijlage 3.2.6: Sexting/sextortion/grooming
- Bijlage 3.2.7: Overig

De resultaten zijn eveneens te raadplegen in Excel- en Word-format. Het eindrapport is hier te raadplegen.
Onderstreepte woorden zijn linkjes naar de betreffende documenten.

Werken de linkjes niet? Mail dan a.u.b. naar e.land@saxion.nl of r.spithoven@saxion.nl

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

↩ Terug naar de inhoudsopgave

4.1 TOELICHTING VOORAF

In dit hoofdstuk wordt de inventarisatie van interventies uit de praktijkgerichte literatuur besproken. Deze inventarisatie is opgesteld door eerst een lijst op te stellen van relevante actoren (denk aan de politie zelf, maar ook Nederlandse Vereniging van Banken, Vereniging van Nederlandse Gemeenten, Stichting Internet Domeinregistratie Nederland, en meer) binnen de aanpak van online criminaliteit, om vervolgens binnen hun websites en databases te zoeken naar relevante interventies.

Duidelijk is geworden dat er veel interventies op het gebied van online criminaliteit en het voorkomen van slachtoffer- en daderschap zijn. Daarom is het bij het raadplegen van de resultaten, belangrijk om in het achterhoofd te houden dat het *geen uitputtende lijst* betreft. De inventarisatie is opgesteld vanaf eind september 2024. In overleg met de opdrachtgever is eind januari 2025 besloten om over te gaan tot rapportage. Het uiteindelijke resultaat betreft een inventarisatie van **35 interventies op het gebied van daderschap**, en **86 interventies op het gebied van slachtofferschap van online criminaliteit.**

Binnen het onderzoek is speciaal aandacht besteed aan de werking van de interventies. Daarom is er specifiek gekeken naar eventueel beschikbare evaluaties en de resultaten hieruit. Omdat er slechts voor enkele interventies evaluaties van goede kwaliteit beschikbaar waren, zijn er nog relatief veel interventies in de inventarisatie opgenomen die geëvalueerd zijn. Opvallend was echter dat dit over het algemeen weinig leek te worden gedaan.

De resultaten van de inventarisatie zijn, zowel in de inventarisatie zelf als in deze eindrapportage, in de volgende categorieën onderverdeeld:

Geëvalueerd, positief resultaat	De interventie heeft de gewenste effecten bereikt, en deelnemers zijn tevreden.
Geëvalueerd, negatief resultaat	De interventie heeft geen/niet de gewenste effecten bereikt en deelnemers waren niet tevreden.
Geëvalueerd, gemixte resultaten	De interventie is min of meer succesvol geweest of het is lastig te meten – daarnaast zijn deelnemers overwegend positief.
Niet geëvalueerd, werking onbekend	Er is geen evaluatie gevonden en het is onduidelijk of de interventie de gewenste effecten heeft gehad.
Niet geëvalueerd, wel veelbelovend/ positieve signalen	De interventie is niet geëvalueerd, maar is wel gebaseerd op praktische en/of wetenschappelijke kennis, is opgesteld in samenwerking met relevante actoren uit de praktijk en/of wetenschap en er worden positieve dingen over gezegd.

↩ Terug naar de overzichtspagina van dit hoofdstuk

Naast een onderverdeling op het gebied van kwaliteit en evaluatie, is er ook een onderverdeling gemaakt op een aantal andere aspecten. Deze zijn als labels in de tabellen geplaatst. De categorieën “Delictstype” en “Doelgroep” spreken voor zich, maar de categorie “Aard van de interventie” wellicht niet. Daarom wordt deze categorie, inclusief de hiervoor gebruikte labels, hieronder kort toegelicht.

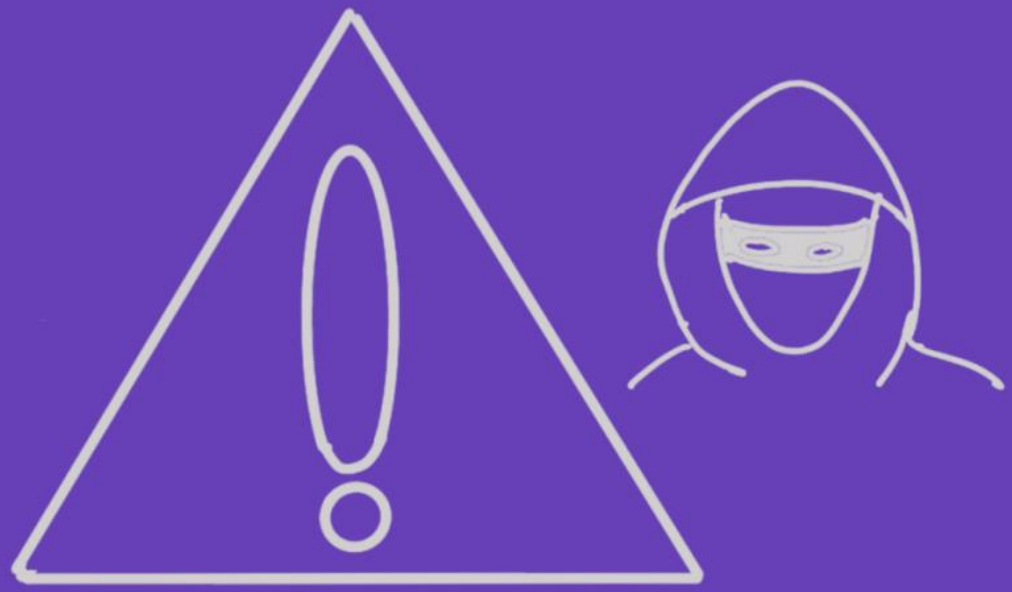
In de categorie “Aard van de interventie” wordt er een onderverdeling gemaakt in de *soort* interventie. Denk hierbij aan interventies specifiek gericht op het uitwisselen en/of delen van informatie, het ondersteunen van de deelnemers/ontvangers en het verstoren van het strafbare gedrag. Onderstaande labels zijn in deze categorie toegepast:

1. **Bewustwordingscampagne**: een campagne geheel ingericht om mensen bewust te maken van een fenomeen of probleem.
2. **Bijeenkomst/evenement**: een interventie waarbij mensen bij elkaar komen om het over het onderwerp/fenomeen te hebben, om met elkaar in discussie te gaan of om activiteiten uit te voeren.
3. **Informatie/educatie**: dit label wordt gegeven aan interventies die zijn gericht op het verschaffen van informatie. Dit kan op allerlei manieren, bijvoorbeeld door middel van een gastles, een cursus of workshop, of simpelweg door een informatie-punt in te richten.
4. **Meldpunt**: een interventie waarop mensen melding kunnen doen wanneer zij een bepaald probleem hebben of online criminaliteit hebben meegemaakt (bijvoorbeeld wanneer ze online zijn opgelicht).
5. **Ondersteuning/hulp**: hierbij gaat het over interventies waarmee ondersteuning of hulp aan hun doelgroep wordt aangeboden. Voorbeelden van soorten interventies die dit label hebben gekregen, zijn toolkits, op maat gemaakte tips/rapporten over de stand van zaken (bijvoorbeeld na een scan op het gebied van cybersecurity) en verwijzingen naar hulpinstanties.
6. **Scan**: een interventie waarbij wordt gekeken naar de doelgroep (meestal zijn dit bedrijven of instanties gebleken) en hoe het er bij deze doelgroep bij staat (op gebied van cybersecurity en -weerbaarheid, onder andere).
7. **Serious game**: een interventie waarmee op een speelse manier kennis wordt overgebracht.
8. **Tool**: dit label is gebruikt voor interventies die door de doelgroep zelf kunnen worden ingezet. Denk hierbij bijvoorbeeld aan een database die kan worden geraadpleegd om te zien of je met een oplichter te maken hebt, of om te zien of jouw gegevens in een datalek voorkomen.
9. **Verstoring**: dit laatste label is toegepast bij interventies die zijn ingericht om een einde te maken aan iemands daderschap.

In dit hoofdstuk worden de resultaten voor slachtoffer- en daderschap over het algemeen weergegeven. De resultaten, gesorteerd per delictstype, zijn in bijlage 3 te vinden. Het eindrapport voor dit onderzoek afzonderlijk, is hiernaast als pdf te downloaden.

PDF

↩ Terug naar de overzichtspagina van dit hoofdstuk



PARAGRAAF 4.2

Inventarisatie bestaande interventies: gericht op daderschap van online criminaliteit

Totaaloverzicht en gesorteerd

4.2 BEVINDINGEN PRAKTISCHE LITERATUUR

DADERSCHAP | Totaaloverzicht van 35 interventies

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | TOTAALOVERZICHT			
Kwaliteit	**Aard van de interventies**	**Delictstype**	**Doelgroepen**
Geen evaluatie, wel succesvol/ veelbelovend = 18x Geen evaluatie, werking onbekend = 8x Geëvalueerd, gemixte reacties = 5x Geëvalueerd, positief resultaat = 4x Geëvalueerd, negatief resultaat = 0x	Informatie/educatie = 18x* Verstoring = 15x Bewustwordings-campagne = 7x Ondersteuning/hulp = 6x Serious game = 6x Evenement/ bijeenkomst = 2x Tool = 1x	Online fraude = 14x ▪ Geldezels = 7x ▪ Aan-/verkoopfraude = 5x ▪ (Bank)helpdeskfraude = 4x ▪ Hulpvraag-/VIN-fraude = 2x ▪ ID-fraude = 2x ▪ Oplichting algemeen = 1x Hacking = 9x Online geweld/cyberpesten = 7x Algemene weerbaarheid = 6x Sextortion/strafbare sexting = 6x Phishing = 3x DDoS = 2x Overig (elk 1x) = ▪ Desinformatie, Exposen, Mal-/ransomware	Jongeren = 21x Algemeen = 14x

*Sommige van de interventies over online fraude gebruikten meerdere, verschillende vormen van fraude in hun concrete voorbeelden. Daarom is het aantal keer dat de individuele soorten fraude voorkomen, niet gelijk aan het totaal dat achter online fraude staat. Dit geldt ook voor de hierop volgende dia's.

↩ Terug naar de overzichtspagina van dit hoofdstuk

4.2 BEVINDINGEN PRAKTISCHE LITERATUUR

DADERSCHAP | Totaaloverzicht 35 interventies gesorteerd | 1/2

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | TOTAAL GESORTEERD			
Kwaliteit	**Aard van de interventies**	**Delictstype**	**Doelgroepen**
Geëvalueerd, positief resultaat *Totaal = 5*	▪ Verstoring = 4x ▪ Bewustwordingscampagne = 1x ▪ Informatie/educatie = 1x ▪ Ondersteuning/hulp = 1x ▪ Serious game = 1x	▪ Online fraude = 4x ○ Aan- en verkoopfraude = 2x ○ Geldezels = 2x ○ (Bank)helpdeskfraude = 1x ○ Hulpvraag- en vriend-in-noodfraude = 1x ▪ Algemene weerbaarheid = 1x ▪ Online geweld/cyberpesten = 1x	▪ Algemeen = 3x ▪ Jongeren = 2x
Geëvalueerd, negatief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, gemixte resultaten *Totaal = 5*	▪ Verstoring = 3x ▪ Informatie/educatie = 1x ▪ Ondersteuning/hulp = 1x ▪ Serious game = 1x	▪ Online fraude = 3x ○ Aan- en verkoopfraude = 2x ○ Geldezels = 1x ▪ Algemene weerbaarheid = 2x ▪ Exposen = 1x ▪ Hacking = 1x ▪ Online geweld/cyberpesten = 1x ▪ Desinformatie = 1x	▪ Jongeren = 3x ▪ Algemeen = 2x

1/2

↩ Terug naar de overzichtspagina van dit hoofdstuk

4.2 BEVINDINGEN PRAKTISCHE LITERATUUR

DADERS | Totaal: gesorteerd

DADERSCHAP | Totaaloverzicht 35 interventies gesorteerd | 2/2

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | TOTAAL GESORTEERD			
Kwaliteit	**Aard van de interventies**	**Delictstype**	**Doelgroepen**
Niet geëvalueerd, werking onbekend *Totaal = 8*	▪ Informatie/educatie = 7x ▪ Serious game = 3x ▪ Bewustwordingscampagne = 2x ▪ Ondersteuning/hulp = 1x	▪ Online geweld/cyberpesten = 4x ▪ Algemene weerbaarheid = 3x ▪ Hacking = 3x ▪ Online fraude = 2x ○ (Bank)helpdeskfraude = 1x ○ Geldezels = 1x ▪ Phishing = 1x ▪ Sextortion/strafbare sexting = 1x	▪ Jongeren = 8x
Niet geëvalueerd, wel veelbelovend/ positieve signalen *Totaal = 17*	▪ Informatie/educatie = 9x ▪ Verstoring = 8x ▪ Bewustwordingscampagne = 4x ▪ Ondersteuning/hulp = 3x ▪ Evenement/bijeenkomst = 2x ▪ Serious game = 1x ▪ Tool = 1x	▪ Hacking = 5x ▪ Online fraude = 5x ○ Geldezels = 3x ○ (Bank)helpdeskfraude = 2x ○ ID-fraude = 2x ○ Aan-/verkoopfraude = 1x ○ Hulpvraag-/vriend-in-noodfraude = 1x ○ Oplichting algemeen = 1x ▪ Sextortion/strafbare sexting = 5x ▪ DDoS = 2x ▪ Mal-/ransomware = 1x ▪ Online geweld/cyberpesten = 2x ▪ Phishing = 2x	▪ Algemeen = 9x ▪ Jongeren = 8x

2/2

↩ Terug naar de overzichtspagina van dit hoofdstuk

PARAGRAAF 4.3

Inventarisatie bestaande interventies: gericht op slachtofferschap van online criminaliteit

Totaaloverzicht en gesorteerd

4.3 BEVINDINGEN PRAKTISCHE LITERATUUR

SLACHTOFFERSCHAP | Totaaloverzicht van 86 interventies

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | TOTAALOVERZICHT

Kwaliteit	Aard van de interventies	Delictstype	Doelgroepen
Geen evaluatie, wel succesvol/ veelbelovend = 28x Geen evaluatie, werking onbekend = 26x Geëvalueerd, positief resultaat = 16x Geëvalueerd, gemixte reacties = 13x Geëvalueerd, negatief resultaat= 3x	Informatie/educatie = 58x Ondersteuning/hulp = 36x Bewustwordings-campagne = 19x Serious game = 19x Tools = 15x Scan = 6x Evenement/ bijeenkomst = 5x Verstoring = 4x Meldpunt = 2x	Algemene weerbaarheid = 41x Online fraude = 34x ▪ Oplichting algemeen = 10x ▪ (Bank)helpdeskfraude = 9x ▪ Hulpvraag-/vriend-in-noodfraude = 9x ▪ Geldezels = 6x ▪ Aan-/verkoopfraude = 5x ▪ Datingfraude = 5x ▪ ID-fraude = 5x ▪ Beleggingsfraude = 1x Hacking = 20x Phishing = 19x Mal-/ransomware = 11x Sextortion/strafbare sexting = 9x Online geweld/cyberpesten = 4x Desinformatie = 3x Overig (elk 1x) = • DDoS , Doxing, Exposen, Hate speech	Algemeen = 33x Jongeren = 24x Bedrijven/ ondernemers = 15x Senioren = 5x Gemeenten = 3x Overig (elk 1x)= ▪ Agrarische sector, Alleenstaanden, Digitaal minder vaardigen, Drinkwatersector, Kwetsbaren algemeen, Laaggeletterden

↩ Terug naar de overzichtspagina van dit hoofdstuk

4.3 BEVINDINGEN PRAKTISCHE LITERATUUR

SLACHTOFFERS | Totaal: gesorteerd

SLACHTOFFERSCHAP | Totaaloverzicht van 86 interventies gesorteerd | 1/2

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | TOTAAL GESORTEERD

Kwaliteit	Aard van de interventies	Delictstype	Doelgroepen
Geëvalueerd, positief resultaat *Totaal = 16*	▪ Ondersteuning/hulp = 9x ▪ Informatie/educatie = 8x ▪ Scan = 5x ▪ Bewustwordingscampagne = 3x ▪ Tool = 3x ▪ Verstoring = 2x ▪ Serious game = 1x	▪ Algemene weerbaarheid = 8x ▪ Online fraude = 6x ○ (Bank)helpdeskfraude = 3x ○ Datingfraude = 2x ○ Aan-/verkoopfraude = 1x ○ Geldezels = 1x ○ Hulpvraag-/vriend-in-noodfraude = 1x ▪ Hacking = 2x ▪ Phishing = 2x ▪ Mal-/ransomware = 1x	▪ Algemeen = 5x ▪ Bedrijven/ ondernemers = 5x ▪ Jongeren = 3x ▪ Senioren = 2x ▪ Gemeenten = 1x ▪ Overig (elk 1x) = ○ Agrarische sector, Kwetsbaren, Alleenstaanden
Geëvalueerd, negatief resultaat *Totaal = 3*	▪ Bewustwordingscampagne = 1x ▪ Informatie/educatie = 1x ▪ Ondersteuning/hulp = 1x ▪ Serious game = 1x	▪ Algemene weerbaarheid = 1x ▪ Desinformatie = 1x ▪ Hacking = 1x	▪ Algemeen = 1x ▪ Bedrijven/ ondernemers = 1x ▪ Jongeren = 1x
Geëvalueerd, gemixte resultaten *Totaal = 13*	▪ Informatie/educatie = 9x ▪ Ondersteuning/hulp = 8x ▪ Bijeenkomst/evenement = 2x ▪ Serious game = 2x ▪ Bewustwordingscampagne = 1x ▪ Scan = 1x	▪ Algemene weerbaarheid = 11x ▪ Online fraude = 4x ○ (Bank)helpdeskfraude = 1x ○ Hulpvraag- en vriend-in-noodfraude = 1x ○ Geldezels = 1x ▪ Phishing = 2x ▪ Overig (elk 1x) = ○ Mal- en ransomware, hacking, online geweld/ cyberpesten, desinformatie, exposen, DDoS	▪ Bedrijven/ ondernemers = 6x ▪ Algemeen = 5x ▪ Jongeren = 3x ▪ Gemeenten = 2x ▪ Senioren = 1x

1/2

↩ Terug naar de overzichtspagina van dit hoofdstuk

4.3 BEVINDINGEN PRAKTISCHE LITERATUUR

SLACHTOFFERSCHAP | Totaaloverzicht van 86 interventies gesorteerd | 2/2

SLACHTOFFERS | Totaal: gesorteerd

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | TOTAAL GESORTEERD

Kwaliteit	Aard van de interventies	Delictstype	Doelgroepen
Niet geëvalueerd, werking onbekend *Totaal = 26*	▪ Informatie/ educatie = 19x ▪ Bewustwordings- campagne = 8x ▪ Serious game = 8x ▪ Ondersteuning/ hulp = 7x ▪ Tool = 6x ▪ Verstoring = 1x ▪ Evenement/ bijeenkomst = 1x	▪ Algemene weerbaarheid = 10x ▪ Online fraude = 10x ○ Oplichting algemeen = 5x ○ Hulpvraag-/vriend-in-noodfraude = 4x ○ Aan-/verkoopfraude = 3x ○ (Bank)helpdeskfraude = 2x ○ Datingfraude = 2x ○ ID-fraude = 2x ○ Beleggingsfraude = 1x ○ Geldezels = 1x ▪ Hacking = 9x ▪ Mal-/ransomware = 7x ▪ Phishing = 6x ▪ Online geweld/cyberpesten = 2x ▪ Sextortion/strafbare sexting = 2x	▪ Algemeen = 14x ▪ Jongeren = 8x ▪ Bedrijven/ ondernemers = 5x ▪ Senioren = 2x ▪ Gemeenten = 1x ▪ Overig (elk 1x) = ○ Drinkwatersector, Laaggeletterden
Niet geëvalueerd, wel veelbelovend/ positieve signalen *Totaal = 28*	▪ Informatie/ educatie = 21x ▪ Ondersteuning/ hulp = 11x ▪ Serious game = 7x ▪ Bewustwordings- campagne = 6x ▪ Tool = 6x ▪ Evenement/ bijeenkomst = 2x ▪ Meldpunt = 2x ▪ Verstoring = 1x	▪ Online fraude = 14x ○ Oplichting algemeen = 5x ○ (Bank)helpdeskfraude = 3x ○ Geldezels = 3x ○ Hulpvraag-/vriend-in-noodfraude = 3x ○ ID-fraude = 3x ○ Datingfraude = 1x ○ Aan-/verkoopfraude = 1x ▪ Algemene weerbaarheid = 11x ▪ Phishing = 9x ▪ Hacking = 7x ▪ Sextortion/sexting/grooming = 7x ▪ Mal-/ransomware = 2x ▪ Overig (elk 1x) = ○ Doxing, Hate speech, Nepnieuws, Online geweld/cyberpesten	▪ Algemeen = 13x ▪ Jongeren = 12x ▪ Bedrijven/ ondernemers = 4x ▪ Senioren = 1x ▪ Gemeenten = 1x ▪ Overig (elk 1x) = ○ Digitaal minder vaardigen

2/2

↩ Terug naar de overzichtspagina van dit hoofdstuk

Afbeelding: Stockfoto

HOOFDSTUK 5

Overkoepelende inzichten per delictsvorm en als totaaloverzichten

Elmira Land BA & dr. Remco Spithoven

Lectoraat Online Weerbaarheid, Hogeschool Saxion.

OPBOUW HOOFDSTUK

HOOFDSTUK 5: OVERKOEPELENDE INZICHTEN Overkoepelende inzichten uit de systematische review, de praktijk, de scoping review en de grijze literatuur, op gebied van dader- en slachtofferschap, per delictsvorm en als totaaloverzichten	
5.1: Toelichting vooraf	
5.2: Daderschap: per delictstype 5.2.1: Online fraude 5.2.2: Hacking 5.2.3: Mal-/ransomware 5.2.4: Sexting/exposen/sextortion 5.2.5: Cyberstalking 5.2.6: *Algemeen*	5.4: Slachtofferschap: per delictstype 5.4.1: Online fraude 5.4.2: Datingfraude 5.4.3: Phishing 5.4.4: *Algemeen*
5.3: Daderschap totaaloverzicht	5.5: Slachtofferschap totaaloverzicht

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

↩ Terug naar de inhoudsopgave

5.1 TOELICHTING VOORAF

In dit hoofdstuk worden de inzichten uit alle onderzoeken die in dit eindrapport besproken zijn (de systematische review, de praktijksessie, de scoping review van wetenschappelijke literatuur en de inventarisatie van praktijkgerichte literatuur over de bestaande interventies) samengenomen in een overzicht van overkoepelende resultaten.

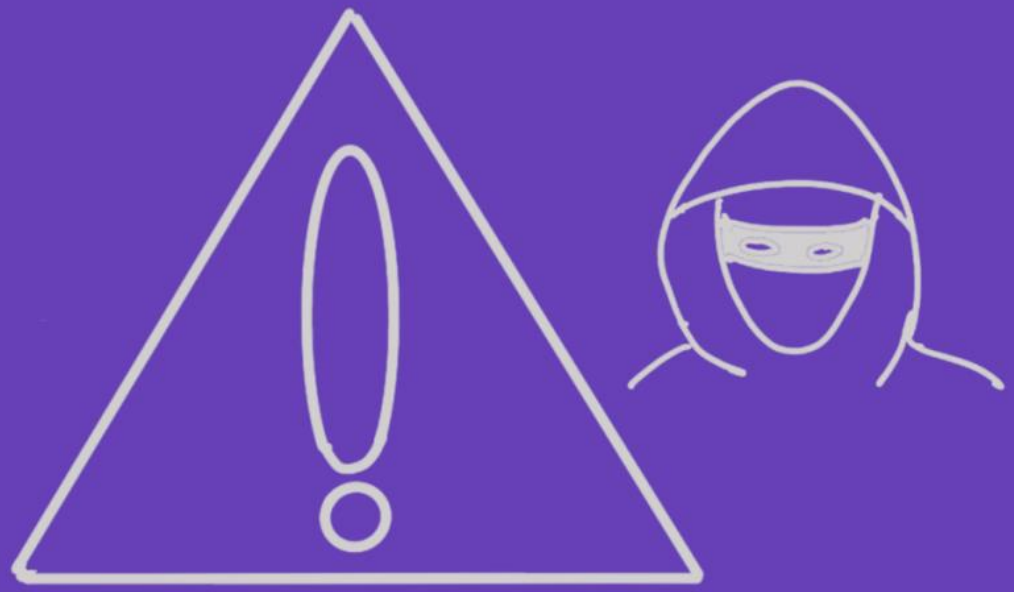
Zoals ook in de voorgaande dia staat weergegeven, worden eerst de overkoepelende conclusies uit de onderzoeken naar daderschap van online criminaliteit weergegeven. Dit wordt eerst algemeen gedaan, en vervolgens per delictstype. Hierna wordt hetzelfde gedaan voor de resultaten met betrekking tot slachtofferschap van online criminaliteit.

De resultaten worden onderverdeeld in de volgende categorieën:

1. **Risicofactoren**: welke factoren hebben invloed op het ontstaan van dader- of slachtofferschap van online criminaliteit? (zie voor meer informatie ook hoofdstuk 1).
   - **Positieve relatie:** hoe meer iemand dit kenmerk heeft of dit gedrag vertoont, hoe groter de kans dat hij of zij dader of slachtoffer wordt.
   - **Negatieve relatie:** hoe meer iemand dit kenmerk heeft of dit gedrag vertoont, hoe kleiner de kans dat hij of zij dader of slachtoffer wordt.
   - **Ambigue** relatie: het is onduidelijk wat de invloed van dit kenmerk of dit gedrag is op dader- of slachtofferschap.
2. **Interventies/trainingen**: wat is er in de onderzoeken naar voren gekomen over interventies en trainingen die ter voorkoming van slachtoffer- en/of daderschap worden ingezet? En waar richten deze interventies zich op? De resultaten in deze categorie komen vooral uit de systematische review en de praktijkgerichte literatuur.
3. **Doelgroepen**: op welke doelgroepen richten de gevonden onderzoeken/interventies/trainingen zich met name? Dit kan gaan over jongeren, senioren, ondernemers en gemeenten, maar ook “algemeen”. Algemeen is als categorie gebruikt indien interventies zich niet op een specifieke doelgroep richten, maar hopen zo veel mogelijk mensen aan te spreken/te helpen.

Op elke dia staat voor het overzicht een legenda weergegeven, waarmee duidelijk wordt uit welk onderzoek de resultaten komen.

↩ Terug naar de overzichtspagina van dit hoofdstuk



PARAGRAAF 5.2

Overkoepelende inzichten: daderschap online criminaliteit

Overzicht per delictstype

5.2.1 OVERKOEPELENDE INZICHTEN PER DELICTSTYPE

DADERSCHAP | Online criminaliteit 1/6 | Online fraude

RISICOFACTOREN | DADERSCHAP | ONLINE FRAUDE		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Praktijksessie ▪ Digitale kennis ▪ (Confrontatie op) sociale media ▪ Slechte financiële positie ▪ Deviante vrienden ▪ Gedwongen criminele carrière na eerste stappen als (bijvoorbeeld) geldezel ▪ Social engineering ▪ Cultuur ▪ Verwevenheid traditionele criminaliteit ▪ Verplaatsing naar dark web ▪ Status en idolen (influencers)	**Praktijksessie** ▪ Leeftijd ▪ Ontwikkeling hersenen ▪ Impuls-onderdrukking ▪ Opleidingsniveau ▪ Ouderlijk toezicht ▪ Idolen (influencers) ▪ Pakkans	**Scoping review** ▪ Netwerk (actoren) ▪ Netwerk (structuur) ▪ COVID-19 pandemie ▪ Obstakels door opsporing en vervolging
Scoping review ▪ Gedeelde banden en gemeenschappelijke affiliaties ▪ Groepsinteractie ▪ Mentorschap ▪ Ouders ▪ Internetgebruik ▪ Neutralisatie bij ouders van fraudeurs ▪ Financieel gewin ▪ Hebzucht ▪ Anticiperen ▪ Samenwerking corrupte overheidsfunctionarissen ▪ Smurfen ▪ Technologie ▪ Verliesaversie ▪ Autoriteit ▪ Schaarste ▪ Urgentie ▪ Afwezigheid capabele bewaker	**Scoping review** ▪ Welvaart	

* +-icoontje staat voor een positieve werking

INTERVENTIES/TRAININGEN	DOELGROEPEN
Praktijksessie ▪ Webinar	**Praktijkgerichte literatuur** ▪ Algemeen ▪ Jongeren
Scoping review + Detectie en monitoren* + Documenteren aard en omvang fraude + Evaluatie maatregelen + Ondersteuning slachtoffers + Impact verkleinen bij slachtoffers + Fraudebestrijdingsplan bij toekomstige crisis + Armoedebestrijding + Gezins- en sociale omgeving + Strikte en onvermijdelijke straffen + Aanpakken van neutralisaties en rationalisaties	
Praktijkgerichte literatuur ▪ Verstoring ▪ Voorbeelden: #Selfmade? Cellmate!, Cyber24, Shitzooi en #Don'tBeAMule + EMMA	

↩ Terug naar de overzichtspagina van dit hoofdstuk

5.2.2 OVERKOEPELENDE INZICHTEN PER DELICTSTYPE

DADERSCHAP | Online criminaliteit 2/6 | Hacking

RISICOFACTOREN | DADERSCHAP | HACKING		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Systematische review ▪ Geslacht (man) ▪ Opleidingsniveau ▪ Sociaal Economische Status ▪ Middelengebruik/ verslaving ▪ Motivatie ▪ Neutralisatietechnieken ▪ Deviante vrienden en social learning ▪ Computer- en internetgebruik ▪ Daderschap overige delicten	**Systematische review** ▪ Leeftijd ▪ Moraliteit ▪ Zelfcontrole ▪ Ouderlijk toezicht	**Systematische review** ▪ Andere etniciteit (non-Kaukasisch) ▪ Werk ▪ ASS gerelateerde kenmerken ▪ IT- en computerkennis & -vaardigheden ▪ Persoonlijkheids-kenmerken ▪ Band met ouders ▪ Sociale banden
Praktijksessie ▪ Relatie tot slachtoffer ▪ Werk gerelateerd aan IT		
Scoping review ▪ Geslacht en leeftijd ▪ Strafblad en recidive ▪ Peers ▪ Neutralisatietechnieken algemeen ▪ Hogere morele principes ▪ Ontkennen van slachtofferschap ▪ Rechtvaardigingsclaim ▪ Veroordelaars veroordelen ▪ Verspreiding van schuld ▪ Game-items ▪ Plezier en impulsiviteit ▪ Woede ▪ Gebruikte kanalen ▪ Koopbaarheid van persoonsgegevens ▪ Persoonlijke informatie ▪ Frequentie	**Scoping review** ▪ Persoonlijke rechtvaardiging ▪ Relatie tot het slachtoffer	**Scoping review** ▪ Chatrooms ▪ Ontkennen van schade ▪ Persoonlijke rechtvaardiging ▪ Rechtvaardiging door vergelijking ▪ Rechtvaardiging o.b.v. noodzaak ▪ Verantwoordelijkheid ontkennen

* +-icoontje staat voor een positieve werking
±-icoontje staat voor een ambigue werking

INTERVENTIES/TRAININGEN	DOELGROEPEN
Praktijksessie ▪ Beveiligen betaalaccounts ▪ Inlichten consumenten ▪ Deter, divert, degrade, disrupt ▪ COPS ▪ Voorbeelden: Hack_Right en Re_B00TCMP	**Praktijkgerichte literatuur** ▪ Jongeren
Scoping review + Monitoren* + Bewustzijn schade + Neutralisatietechnieken ± Afschrikking	
Praktijkgerichte literatuur ▪ Informatie/educatie ▪ Evenement/bijeenkomst ▪ Voorbeelden: Hack_Right, Cyber24, re_B00TCMP en Cyber Choices	

↩ Terug naar de overzichtspagina van dit hoofdstuk

5.2.3 OVERKOEPELENDE INZICHTEN PER DELICTSTYPE

DADERSCHAP | Online criminaliteit 3/6 | Mal-/ransomware

RISICOFACTOREN | DADERSCHAP | MAL-/RANSOMWARE		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Systematische review ▪ ASS gerelateerde kenmerken ▪ IT en computerkennis & -vaardigheden ▪ Neutralisatietechnieken ▪ Deviante vrienden en social learning	**Systematische review** ▪ Persoonlijkheids-kenmerken ▪ Cognitieve vaardigheden	**Systematische review** ▪ Geslacht (man) ▪ Online routine activiteiten
Praktijksessie ▪ Competitiegedrag tussen daders	**Praktijksessie** ▪ Vormen van toezicht ▪ Financiën	
Scoping review ▪ Internetgebruikers ▪ Blokkeren van toegang ▪ Social engineering ▪ Verspreiding via download of bijlage in e-mails	**Scoping review** ▪ Welvaart	

INTERVENTIES/TRAININGEN	DOELGROEPEN
Praktijksessie ▪ Infiltratie in hackfora ▪ Vroegsignalering ▪ Maatschappelijke stage IT-bedrijf ▪ Neutraliseren neutralisatie-technieken ▪ Pakkans vergroten	-

↩ Terug naar de overzichtspagina van dit hoofdstuk

5.2.4 OVERKOEPELENDE INZICHTEN PER DELICTSTYPE

DADERSCHAP | Online criminaliteit 4/6 | Sexting/exposen/sextortion

DADERS	Sexting/ exposen/ sextortion

RISICOFACTOREN | DADERSCHAP | SEXTING/EXPOSEN/SEXTORTION		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Systematische review ▪ Geslacht (man) ▪ Opleidingsniveau ▪ Houding t.o.v. sexting	**Systematische review** ▪ Persoonlijkheids-kenmerken ▪ Groepsdruk en peergroep	-
Praktijksessie ▪ Relatie tot slachtoffer ▪ Autisme ▪ Groepsdruk ▪ Wens voor macht/controle	**Praktijksessie** ▪ Empathisch vermogen ▪ Denkbeeld over vrouwen ▪ Seksuele tevredenheid	

INTERVENTIES/TRAININGEN	DOELGROEPEN
Praktijksessie ▪ Meer toezicht ▪ Lessen over impact ▪ Uitleg over ongecontroleerde verspreiding ▪ Privaatrechtelijke aansprakelijkheid	**Praktijksessie** ▪ Jongeren
Praktijkgerichte literatuur ▪ Informatie/educatie ▪ Voorbeelden: Shitzooi, Respect Online (van Halt.) en Toolkit L.O.V.E. Online (ook van Halt.)	**Praktijkgerichte literatuur** ▪ Jongeren

↩ Terug naar de overzichtspagina van dit hoofdstuk

5.2.5 OVERKOEPELENDE INZICHTEN PER DELICTSTYPE

DADERSCHAP | Online criminaliteit 5/6 | Cyberstalking

RISICOFACTOREN | DADERSCHAP | CYBERSTALKING		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Systematische review ▪ Etniciteit ▪ Geslacht (man) ▪ Opleidingsniveau ▪ Middelengebruik/verslaving ▪ Persoonlijkheidskenmerken ▪ Risicogedrag ▪ Geestelijke gezondheidsproblemen ▪ Deviante vrienden en social learning ▪ Computer- en internetgebruik ▪ Daderschap offline criminaliteit ▪ Daderschat online criminaliteit ▪ Eerder slachtofferschap	**Systematische review** ▪ Hechtingsproblemen ▪ Sociale steun	**Systematische review** ▪ Cultuur
Praktijksessie ▪ LVB ▪ Autisme ▪ Deviante vrienden ▪ Middelengebruik ▪ Relatie dader-slachtoffer	**Praktijksessie** ▪ Onderdeel uitmaken van de samenleving	

INTERVENTIES/TRAININGEN	DOELGROEPEN
Praktijksessie ▪ Niet-strafrechtelijke interventies ▪ Online gebiedsverbod	-

↩ Terug naar de overzichtspagina van dit hoofdstuk

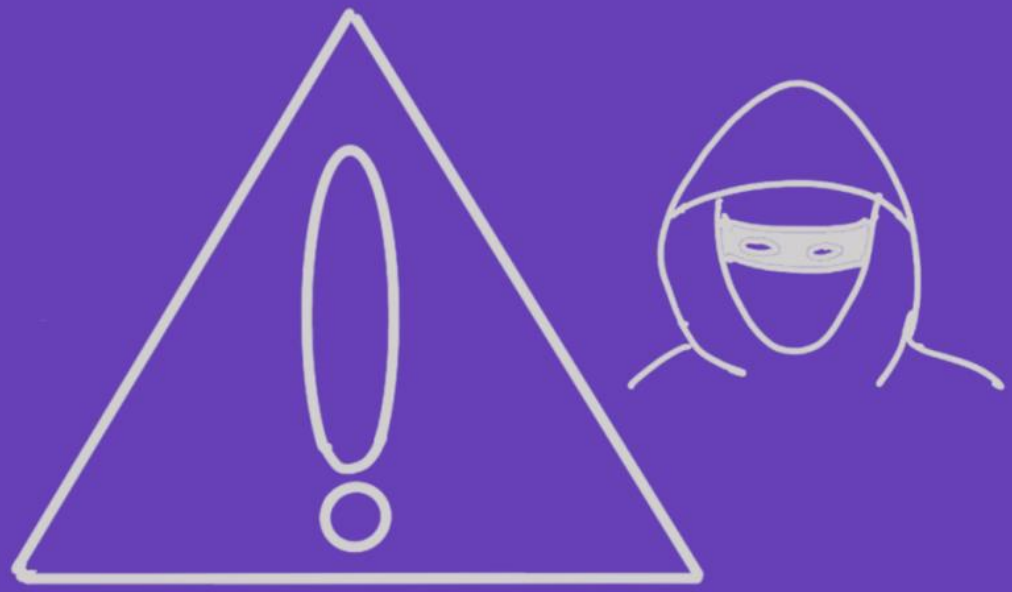
5.2.6 OVERKOEPELENDE INZICHTEN PER DELICTSTYPE

DADERSCHAP | Online criminaliteit 6/6 | *Algemeen*

RISICOFACTOREN | DADERSCHAP | *ALGEMEEN*		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Systematische review ▪ ASS gerelateerde kenmerken ▪ Motivatie ▪ Zelfcontrole ▪ Deviante vrienden en social learning ▪ Gaming	**Systematische review** ▪ Leeftijd	**Systematische review** ▪ Geslacht (man) ▪ Werk
Praktijksessie ▪ Sociale media ▪ Sociale relaties ▪ IT-kennis	**Praktijksessie** ▪ Rolmodellen in de wijk ▪ Toezicht van ouders	**Praktijksessie** ▪ Geslacht ▪ Statelijke actoren ▪ Gaming

INTERVENTIES/TRAININGEN	DOELGROEPEN
Praktijksessie ▪ Meer afpakken, status wegnemen ▪ Sociale relaties verbeteren ▪ Positief belonen ▪ Aandacht voor technische capaciteit daders ▪ Pakkans vergroten ▪ Koppeling maken zorg en IT ▪ Verbinding leggen, bijvoorbeeld via games ▪ Voorlichting al op basisscholen ▪ Geautomatiseerde signalering ▪ Samenwerking met faciliterende organisaties en actoren ▪ Informatie-uitwisseling ▪ Genoemde voorbeelden: COPS, Junior IOT, Cyberbrein, mijn Cyberrijbewijs, HackShield, Re_b00tcmp en Framed	**Praktijkgerichte literatuur** ▪ Jongeren
Praktijkgerichte literatuur ▪ Serious game ▪ Informatie/educatie ▪ Voorbeelden: Framed, Youth Cyber Team, Cyber Explorers, #BeCyberSmart en NetSmartz	

↩ Terug naar de overzichtspagina van dit hoofdstuk



PARAGRAAF 5.3

Overkoepelende inzichten: daderschap online criminaliteit

Totaaloverzicht

5.3 TOTAALOVERZICHT OVERKOEPELENDE INZICHTEN

DADERSCHAP | Online criminaliteit | *Overkoepelende inzichten 1/2*

RISICOFACTOREN | DADERSCHAP | ONLINE CRIMINALITEIT | *OVERKOEPELENDE INZICHTEN*						
Positieve relatie					**Negatieve relatie**	**Ambigue relatie**
Systematische review ▪ Opleidingsniveau ▪ Geslacht (man) ▪ ASS gerelateerde kenmerken ▪ Middelengebruik/verslaving	▪ Risico's nemen ▪ Motivaties ▪ Neutralisatietechnieken ▪ Deviante vrienden en social learning	▪ Computer- en internetgebruik ▪ Daderschap online criminaliteit			**Systematische review** ▪ Leeftijd	**Systematische review** ▪ Geslacht **Praktijksessie** ▪ Geslacht en leeftijd
Scoping review ▪ Geslacht (man) ▪ Migratiestatus ▪ IT-kennis ▪ Cognitieve bias ▪ Psycho-analytische theorie ▪ Risicogedrag ▪ Space Transition theorie ▪ Stress ▪ Meervoudige dader ▪ Gemeenschap ▪ Groepsdruk ▪ Intimidatie ▪ Peers ▪ Traditioneel en online sociaal leren ▪ Armoede ▪ Cultuur ▪ Maatschappelijke eisen ▪ Migratie	▪ Geslacht (man) ▪ Migratiestatus ▪ IT-kennis ▪ Cognitieve bias ▪ Psycho-analytische theorie ▪ Risicogedrag ▪ Space Transition theorie ▪ Stress ▪ Meervoudige dader ▪ Gemeenschap ▪ Groepsdruk ▪ Intimidatie ▪ Peers ▪ Traditioneel en online sociaal leren ▪ Armoede ▪ Cultuur ▪ Maatschappelijke eisen ▪ Ongelijkheid	▪ Wetgeving en wets-handhaving ▪ Dehumanisering ▪ Digitale ruimte ▪ Economische rechtvaardiging ▪ Hogere loyaliteiten ▪ Koloniaal verleden ▪ Ontkennen van schade ▪ Ontkennen van slachtofferschap ▪ Ontkennen van verantwoordelijkheid ▪ Veroordelen van veroordelaars ▪ Afpersing ▪ Avengers ▪ Disrespect ▪ Financieel gewin ▪ Financiële problemen	▪ Hebzucht ▪ Seksuele uitbuiting ▪ Wraak ▪ AI-technologie ▪ Gebruik van persoonsgegevens ▪ Netwerk ▪ Online platforms ▪ Wisselende MO ▪ Anonimiteit ▪ Corporate crimes ▪ Cryptocurrency ▪ Darknet ▪ Digitaal bewijs ▪ Extravagante levensstijl ▪ Frequentie ▪ Groeiende dreiging ▪ Kant-en-klare tools ▪ Risico van AI		**Scoping review** ▪ Opleidingsniveau ▪ Morele ontwikkeling ▪ Empathie ▪ Zelfcontrole ▪ Ouderschap ▪ Sociale banden ▪ Religieuze overtuigingen	**Scoping review** ▪ Leeftijd ▪ Altruïsme

1/2

↩ Terug naar de overzichtspagina van dit hoofdstuk

5.3 TOTAALOVERZICHT OVERKOEPELENDE INZICHTEN

DADERSCHAP | Online criminaliteit | *Overkoepelende inzichten 2/2*

INTERVENTIES/TRAININGEN	DOELGROEPEN
Praktijksessie ▪ Via scholen van daders weerbaarheidsinstructie inzetten ▪ Aanpak van COPS ▪ Social media inzetten ▪ Offline halen van online groepen/content	**Praktijksessie** ▪ Jongeren
Scoping review + Bewustzijn* + Detectie + Innovatieve methodes + Monitoren + Ondersteuning slachtoffer + Risicobeoordeling + Samenwerking + Wetgeving + Zelfbeschermingsmaatregelen + Cognitieve bias + Ethisch gedrag + Sociaalgerichte interventies + Socio-economische interventie + Verdienmodel	**Praktijkgerichte literatuur** ▪ Jongeren
Praktijkgerichte literatuur ▪ Informatie/educatie ▪ Verstoring	

2/2

* +-icoontje staat voor een positieve werking

↩ Terug naar de overzichtspagina van dit hoofdstuk

PARAGRAAF 5.4

Overkoepelende inzichten: slachtofferschap online criminaliteit

Overzicht per delictstype

5.4.1 OVERKOEPELENDE INZICHTEN PER DELICTSTYPE

SLACHTOFFERS | Online fraude

SLACHTOFFERSCHAP | Online criminaliteit 1/4 | Online fraude

RISICOFACTOREN | SLACHTOFFERSCHAP | ONLINE FRAUDE		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Systematische review ▪ Bezittingen ▪ Autoriteit en legitimiteit ▪ Depressie ▪ Eenvoudige oplossingen ▪ Impulsiviteit ▪ Persoonlijkheidskenmerken ▪ Schaamte ▪ Vaardigheden digitale veiligheid ▪ Vertrouwen in autoriteit ▪ Geheugenproblemen ▪ Internetgebruik ▪ Eenzaamheid en isolement ▪ Stigma	**Systematische review** ▪ Bewustzijn ▪ Cognitieve vaardigheden ▪ IT-kennis ▪ Cognitieve functies ▪ Eerder slachtofferschap ▪ Technologische toegang ▪ Partner	**Systematische review** ▪ Inkomen ▪ Leeftijd ▪ Opleidingsniveau ▪ Fysieke gezondheid ▪ Vertrouwen in anderen
Praktijksessie ▪ Vermogen ▪ Naïviteit/goedgelovigheid ▪ Gevoeligheid voor druk ▪ Schaamte ▪ Kwetsbaarheid ▪ Leeftijd ▪ Eerder slachtofferschap ▪ Social engineering	**Praktijksessie** ▪ Vaardigheden digitale veiligheid ▪ Zelfcontrole	

* - (min) -icoontje staat voor een negatieve werking

INTERVENTIES/TRAININGEN	DOELGROEPEN
Systematische review - Bewustwording* - Weerbaarheid	**Praktijksessie** ▪ Senioren
Praktijksessie ▪ Cyberschaamte doorbreken ▪ Slachtoffer journey als basis voor interventies ▪ Handelingskader per type delict ▪ Naasten betrekken bij preventie ▪ Campagne “Frauderen, zo werkt het!”	
Praktijkgerichte literatuur ▪ Informatie/educatie ▪ Ondersteuning/hulp ▪ Bewustwordingscampagne ▪ Tool ▪ Voorbeelden: Bank voor de Klas, Echt of nep?, #EchtNep? en Cyber24	**Praktijkgerichte literatuur** ▪ Algemeen

↩ Terug naar de overzichtspagina van dit hoofdstuk

5.4.2 OVERKOEPELENDE INZICHTEN PER DELICTSTYPE

SLACHTOFFERSCHAP | Online criminaliteit 2/4 | Datingfraude

SLACHTOFFERS | Datingfraude

RISICOFACTOREN | SLACHTOFFERSCHAP | Datingfraude		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Systematische review ▪ Geslacht (vrouw) ▪ Opleidingsniveau ▪ Impulsiviteit	**Systematische review** ▪ Zelfcontrole ▪ Bewustzijn	**Systematische review** ▪ Neuroticisme ▪ Sensatiezucht
Praktijksessie ▪ Eenzaamheid en isolement ▪ Schaamte ▪ Social engineering ▪ Plichtsgetrouw		**Praktijksessie** ▪ Sociaal netwerk ▪ Geslacht (vrouw)

* - (min) -icoontje staat voor een negatieve werking

INTERVENTIES/TRAININGEN	DOELGROEPEN
Systematische review - Profielherkenning* - Individuele strategie	**Praktijkgerichte literatuur** ▪ Senioren ▪ Algemeen
Praktijksessie ▪ Samenwerking met sociale media bedrijven ▪ Sneller actuele MO's delen met breed publiek ▪ Verstoren gelegenheidsstructuur ▪ Sociaal vangnet creëren ▪ Input psychologen vragen ▪ Barrières in datingapps ▪ Slachtoffers blijven geloven ▪ Voorbeelden: Operation shamrock, operation level up, scène uit film Echt of Nep? VAR	
Praktijkgerichte literatuur ▪ Bewustwordingscampagne ▪ Informatie/educatie ▪ Voorbeelden: Verlies je hart niet aan datingfraude en Verliefd op de persoon? Of op het profiel?	

↩ Terug naar de overzichtspagina van dit hoofdstuk

5.4.3 OVERKOEPELENDE INZICHTEN PER DELICTSTYPE

SLACHTOFFERS | Phishing

SLACHTOFFERSCHAP | Online criminaliteit 3/4 | Phishing

RISICOFACTOREN | SLACHTOFFERSCHAP | PHISHING		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Systematische review ▪ Autoriteit ▪ Heuristieken ▪ Impulsiviteit ▪ Persoonlijkheids-kenmerken ▪ Zelfvertrouwen & zelfgenoegzaamheid	**Systematische review** ▪ Aandachtscontrole ▪ Bewustzijn ▪ Computerkennis/-vaardigheden ▪ Zelfbeheersing	**Systematische review** ▪ Geslacht ▪ Leeftijd ▪ Etniciteit ▪ Internetgebruik ▪ Bedrijfscultuur ▪ Prevalentie effect
Praktijksessie ▪ Schaamte ▪ Uit naam van bekende instantie		

INTERVENTIES/TRAININGEN	DOELGROEPEN
Systematische review + Belonen en straffen* + Klassikale training + Technologische tekorten - Algemeen - Feedback - Games - Gepersonaliseerde training - Herhaling - Ingebedde training - Mobiele applicaties - User interface - Waarschuwingsberichten	**Praktijkgerichte literatuur** ▪ Algemeen ▪ Jongeren
Praktijksessie ▪ Preventie ▪ Notficatie na datalek of –hack ▪ Meer gerichte training/ interventieprogramma's	
Praktijkgerichte literatuur ▪ Informatie/educatie ▪ Ondersteuning/hulp ▪ Voorbeelden: Echt of nep?, Laat je niet interneppen en ScamShield	

* +-icoontje staat voor een positieve werking
- (min) -icoontje staat voor een negatieve werking

↩ Terug naar de overzichtspagina van dit hoofdstuk

5.4.4 OVERKOEPELENDE INZICHTEN PER DELICTSTYPE

SLACHTOFFERSCHAP | Online criminaliteit 4/4 | *Algemeen*

RISICOFACTOREN | SLACHTOFFERSCHAP | *ALGEMEEN*		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Systematische review ▪ Geslacht (vrouw) ▪ Waargenomen risico ▪ Angst ▪ Eerder slachtofferschap ▪ Kenmerken dader ▪ Relatiestatus	-	**Systematische review** ▪ Leeftijd ▪ Etniciteit ▪ Inkomen ▪ Opleiding ▪ Werk ▪ Type criminaliteit ▪ Internetgebruik ▪ Online activiteiten

INTERVENTIES/TRAININGEN	DOELGROEPEN
Praktijkgerichte literatuur ▪ Informatie/educatie ▪ Ondersteuning/hulp ▪ Voorbeelden: CyberSprinters, STOP.THINK.CONNECT., HackShield, Echt niet vandaag en Cyber Explorers	**Praktijkgerichte literatuur** ▪ Ondernemers/ bedrijven ▪ Jongeren

↩ Terug naar de overzichtspagina van dit hoofdstuk

PARAGRAAF 5.5

Overkoepelende inzichten: slachtofferschap online criminaliteit

Totaaloverzicht

5.5 TOTAALOVERZICHT OVERKOEPELENDE INZICHTEN

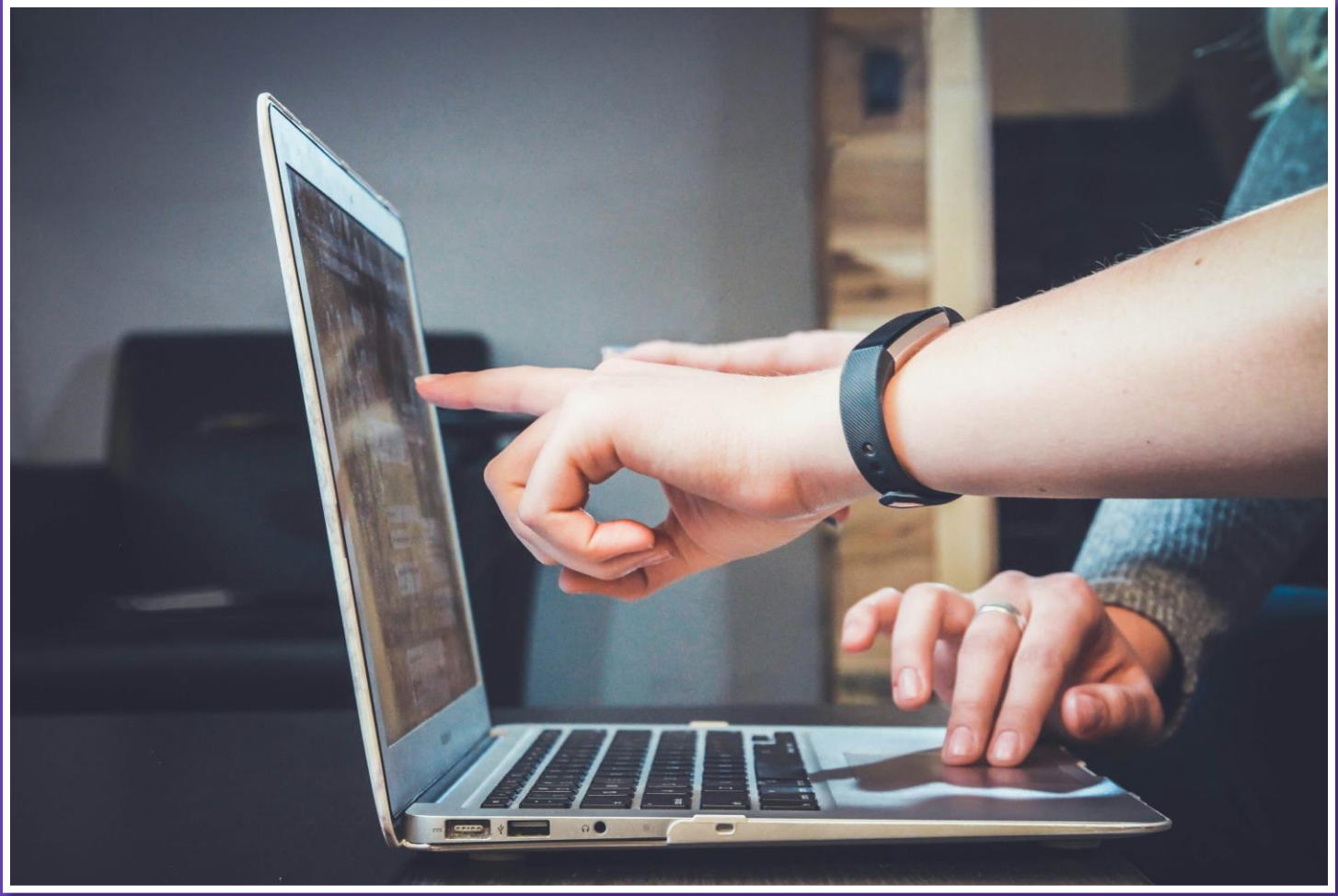
SLACHTOFFERSCHAP | Online criminaliteit | *Overkoepelende inzichten*

SLACHTOFFERS | *Overkoepelende inzichten*

RISICOFACTOREN | SLACHTOFFERSCHAP | ONLINE CRIMINALITEIT | *OVERKOEPELENDE INZICHTEN*		
Positieve relatie	**Negatieve relatie**	**Ambigue relatie**
Systematische review ▪ Geslacht (vrouw) ▪ Gevoelig voor autoriteit	**Systematische review** ▪ Zelfbeheersing ▪ Bewustzijn ▪ IT-kennis en computer-vaardigheden	**Systematische review** ▪ Leeftijd ▪ Opleidingsniveau ▪ Etniciteit ▪ Inkomen
Praktijksessie ▪ Cyberschaamte		**Praktijksessie** ▪ Geslacht ▪ Leeftijd ▪ Omgeving, zoals een “braaf” dorpje ▪ IT-kennis en –vaardigheden

INTERVENTIES/TRAININGEN	DOELGROEPEN
Praktijksessie ▪ Verstoring (van modus operandi en gelegenheidsstructuren) ▪ Meldingsbereidheid vergroten ▪ Cyberschaamte doorbreken ▪ Inzet op preventie en nazorg ▪ Delen van ervaringsverhalen ▪ Detectie en preventiemaatregelen ▪ Gespecialiseerd team voor online slachtofferpreventie ▪ Voorbeelden: Scam Survivors, WhatsNep en Echt Nep?	**Praktijkgerichte literatuur** ▪ Jongeren ▪ Ondernemers/ bedrijven
Praktijkgerichte literatuur ▪ Informatie/educatie ▪ Ondersteuning/hulp	

↩ Terug naar de overzichtspagina van dit hoofdstuk



Afbeelding: Unsplash. (2018, 19 januari). https://unsplash.com/photos/person-using-laptop-FIPc9_VocJ4

HOOFDSTUK 6

Conclusies en aanbevelingen

dr. Remco Spithoven, lector Online Weerbaarheid Hogeschool Saxion

OPBOUW HOOFDSTUK

HOOFDSTUK 6: CONCLUSIES EN AANBEVELINGEN	
1/6:	▪ Eerder gebundelde inzichten over daders ▪ Aanpak van daders volgens professionals
2/6:	▪ Nieuw samengebrachte inzichten over daders
3/6:	▪ Bestaande interventies daders ▪ Kansen voor interventies daders
4/6:	▪ Aanbevelingen onderzoek naar daders ▪ Eerder gebundelde inzichten slachtoffers
5/6:	▪ Kansen voor interventies slachtoffers ▪ Bestaande interventies slachtoffers
6/6:	▪ Aanbevelingen slachtoffers voor praktijk ▪ Vervolgonderzoek slachtoffers

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

↩ Terug naar de inhoudsopgave

CONCLUSIES EN AANBEVELINGEN | 1/6

In dit onderdeel maken we de balans van dit onderzoek op. Op basis van de gestructureerde literatuurstudie werd direct al duidelijk dat er relatief veel inzichten zijn samengebracht rondom daderschap en minder rondom slachtofferschap van online criminaliteit (zowel cybercrime in enge zin als gedigitaliseerde criminaliteit).

[EERDER GEBUNDELDE INZICHTEN OVER DADERS]

Uit de gestructureerde literatuurstudies werd duidelijk dat er relatief veel is samengebracht over daders van cybercrime in enge zin en veel minder over daders van gedigitaliseerde criminaliteit. Over daders van cybercrime in enge zin bestaat het volgende inzicht: het zijn relatief hoog opgeleide jonge mannen met opvallend veel ASS-kenmerken. Zij hebben een primaire, technische motivatie waarmee zij leren veel geld te kunnen verdienen. Daarbij zijn zij sterk gericht op het nemen van risico's en passen zij verschillende neutralisatie-technieken toe waarmee zij hun daderschap voor zichzelf rechtvaardigen. Ook staan zij onder invloed van deviante vrienden en leren zij van elkaar hoe online criminaliteit te plegen. Zij zijn ook daders van minder technische delicten.

[AANPAK VAN DADERS VOLGENS PROFESSIONALS]

Volgens de professionals in de focusgroep moet er meer zicht komen op de invloed van geslacht en leeftijd op daders van online criminaliteit. Daarnaast willen zij meer onderscheid maken in daders van cybercrime in enge zin en daders van gedigitaliseerde criminaliteit. Ook willen zij meer zicht krijgen op daders van veelvoorkomende, gedigitaliseerde criminaliteit en factoren die dit daderschap versterken.

In de aanpak van daders van online criminaliteit zagen de professionals vooral kansen voor samenwerking met en interventies in het onderwijs. Hierbij moet ook nadrukkelijke aandacht zijn voor het onderlinge, sociale leren tussen daders. Daarbij kan worden ingezet op samenwerking met het Cyber Offenders Prevention Squad (COPS) van de Nationale Politie en ziet men kansen voor de inzet van privaatrechtelijke interventies en de preventieve inzet van sociale media.

↩ Terug naar de overzichtspagina van dit hoofdstuk

CONCLUSIES EN AANBEVELINGEN | 2/6

[NIEUW SAMENGEBRACHTE INZICHTEN OVER DADERS]

In de los verschenen, wetenschappelijke artikelen over daders van online criminaliteit die tussen 2021 en 2024 zijn verschenen werd duidelijk dat daders van online criminaliteit overwegend mannen in een achterstandspositie zijn die financiële problemen hebben. Ook worden daders aangetrokken door een luxe levensstijl. Hierbij clusteren zich kenmerken van armoede, een migratieachtergrond en het ervaren van maatschappelijke achterstand. Daders kunnen moeilijk op legitieme wijze meekomen in het maatschappelijke streven naar inkomen en status. Zij komen vaker in contact met wetshandhavers.

Daders handelen vanuit financieel gewin (deels uit financiële problemen), hebzucht maar soms ook uit wraak - mede voor ervaren disrespect - en stellen zich daarbij op als *avengers* (wrekers). Daarbij maken zij gebruik van oplichting, afpersing en seksuele uitbuiting. Om hun daden te rechtvaardigen maken zij gebruik van strategieën als ontmenselijking, de wetteloosheid van de digitale omgeving, economische rechtvaardiging en beroepen zij zich op hogere loyaliteiten of op het slachtofferschap van kolonialisme in de familielijnen. Daarnaast ontkennen zij schade, slachtofferschap en verantwoordelijkheid en veroordelen zij wie hen veroordelen.

Daders maken gebruik van wisselende modus operandi en gebruiken daarin online platformen, (meer en minder gestructureerde) netwerken, persoonsgegevens en AI-technologie. Duidelijk is dat de **sociale relaties** tussen daders van sterke invloed zijn op hun gedrag. Daarbij komen daders vaak uit dezelfde gemeenschap en ervaren zij ook druk vanuit hun *peers* om (online) criminaliteit te plegen. Daarbij kan ook sprake zijn van intimidatie. Overwegend is er vooral sprake van sociaal leren: daders leren van elkaar en dat gebeurt zowel in offline als online settings, van een gesprek op een hangplek of in een woonkamer tot een chatgesprek of uitwisseling van ervaringen op besloten fora.

In deze literatuur wordt duidelijk dat daders van online criminaliteit niet per se over diepgaande IT-kennis beschikken maar deze ook via het internet eigen maken of complete, kant-en-klare pakketten inkopen of aanvullende expertise inkopen. Ook is er een meer algemeen beeld ontstaan van persoonlijkheidskenmerken.

↩ Terug naar de overzichtspagina van dit hoofdstuk

CONCLUSIES EN AANBEVELINGEN | 3/6

Zo blijkt het online daderschap samen te hangen met meer algemeen risicogedrag en is er sprake van meervoudig daderschap: men beperkt zich niet tot een specifiek delict, maar doet wat opportuun is en combineert daarbij online en offline delicten. Ook werd duidelijk dat daders van online criminaliteit een grote mate van stress ervaren en daarnaast problemen ondervinden die samenhangen met cognitief functioneren en psychische problemen. Daarbij vertalen zij – vanuit de *Space Transition* theorie bezien – hun criminele gedrag van de online ook naar de offline omgeving.

Wetenschappers wijzen op de volgende trends: zo is er volgens hen sprake van een groeiende dreiging van online daders als gevolg van een toenemende frequentie in online daderschap, de beschikbaarheid van kant-en-klare tools om online aanvallen te plegen en de risico's van AI-technologie. Daarbij zien zij daders meer professionaliseren in het versterken van hun anonimiteit waarmee digitaal bewijs steeds complexer wordt. Ook zien zij daders opschuiven naar aanvallen op bedrijven en organisaties. Daarnaast zien zij een sterke invloed van het gebruik van cryptocurrencies en activiteiten op het *dark web,* vanwege de hoge mate van anonimiteit.

[BESTAANDE INTERVENTIES DADERS]

Als we naar de bestaande interventies ter preventie en de aanpak van daders in de beschikbare, praktijkgerichte literatuur kijken dan zien we dat er in verhouding tot interventies rondom slachtofferpreventie relatief weinig interventies beschikbaar zijn om daderschap te voorkomen en aan te pakken. Daarbij zijn er maar weinig interventies gericht op daders van specifieke delicten, terwijl daar wel rijke inzichten over beschikbaar zijn. De interventies die er zijn, richten zich vooral op daders van online fraude en de algemene weerbaarheid en deze zijn daarnaast overwegend gericht op verstoring, informeren en educatie. Deze zijn haast uitsluitend gericht op jongeren.

[KANSEN VOOR INTERVENTIES DADERS]

Er liggen goede kansen om de verzamelde inzichten te benutten voor interventies ten aanzien van daders van: online criminaliteit in het algemeen, cybercrime in enge zin, online fraude, phishing/vishing, geldezels en social engineering. Daarbij kan worden geleerd van bestaande interventies door wat werkt toe te passen en wat niet werkt aan te passen.

↩ Terug naar de overzichtspagina van dit hoofdstuk

CONCLUSIES EN AANBEVELINGEN | 4/6

[AANBEVELINGEN ONDERZOEK NAAR DADERS]

- Doe meer gestructureerd literatuuronderzoek naar daders van gedigitaliseerde criminaliteit;
- Doe meer onderzoek naar de mix van daderschap van cybercrime in enge zin, gedigitaliseerde criminaliteit en georganiseerde of ondermijnende criminaliteit ofwel de hybridisering van criminaliteit;
- Doe meer onderzoek naar de rol van cryptocurrencies in modus operandi en witwassen van buitgemaakt geld;
- Doe meer onderzoek naar risicofactoren van daderschap in bredere contexten (steekproefgrootte, landen, situaties, en online delicten) zodat vergelijkingen kunnen worden gemaakt.

[EERDER GEBUNDELDE INZICHTEN SLACHTOFFERS]

Rondom het slachtofferschap viel in de gestructureerde literatuuronderzoeken op dat er relatief veel inzichten zijn samengebracht over slachtofferschap van phishing en relatief minder over slachtofferschap van online fraude (m.u.v. datingfraude), online geweld en cybercrime in enge zin.

Het beeld dat van slachtoffers van – dus met name phishing – bestaat is dat zij gevoelig zijn voor social engineering en dan met name autoriteit. Beschermende factoren zijn daarbij bewustzijn en zelfbeheersing.

Waar in de wetenschap ook geslacht (vrouw zijn) als riscofactor en IT-kennis en computervaardigheden als beschermende factor voor slachtofferschap werden genoemd betwijfelden de professionals deze factoren in de focusgroep. Op basis van hun waarnemingen moet meer worden gezocht naar de invloed van leeftijd, kapitaalkracht en type woonomgeving van slachtoffers van online criminaliteit. Daarbij vermelden zij eveneens een sterke invloed van cyberschaamte: slachtoffers houden hun slachtofferschap verborgen voor hulpverleners, vrienden en familie.

↩ Terug naar de overzichtspagina van dit hoofdstuk

CONCLUSIES EN AANBEVELINGEN | 5/6

[KANSEN VOOR INTERVENTIES SLACHTOFFERS]

De professionals zagen vooral kansen om potentiële slachtoffers in interventies meer gebruik te laten maken van het ‘niet-pluis-gevoel’. Ook zagen zij kansen voor online slachtofferpreventie en het realiseren van integrale slachtofferhulp, van preventieve tot nazorg door samenwerkende publieke en private organisaties. Om de slachtofferverhalen in te kunnen zetten, moet de zogenaamde cyberschaamte worden doorbroken en overall moet de meldings- en aangiftebereidheid onder slachtoffers toenemen.

Tevens worden er mogelijkheden gezien om aan de kant van de slachtoffers gelegenheid te verkleinen door bijvoorbeeld vertragingen in betalingen in te bouwen. Hiervoor kan de modus operandi van verschillende vormen van online criminaliteit worden doorgrond om aanknopingspunten voor verstoring te vinden. Ook kan hierbij met risicoprofielen van slachtoffers worden gewerkt.

[BESTAANDE INTERVENTIES SLACHTOFFERS]

Er bestaan in verhouding tot de interventies rondom daderschap van online criminaliteit relatief veel interventies ter preventie van slachtofferschap. Hiervan zijn ook al de nodige interventies op effect geëvalueerd, waarvan een goed deel ook hun positieve werking hebben bewezen. Deze richten zich vooral op (I) informeren en educatie en (II) het ondersteunen en helpen van slachtoffers.

De focus ligt in de bestaande interventies overwegend op het versterken van de algemene weerbaarheid en preventie van slachtofferschap van online fraude. De doelgroepen zijn daarbij respectievelijk bedrijven, ondernemers, jongeren en het algemene publiek. Relatief weinig geëvalueerde interventies zijn gericht op senioren en specifieke sectoren van bedrijven en ondernemers. Er zijn weinig tot geen positief geëvalueerde interventies die zich richten op de preventie van slachtofferschap van cybercrime in enge zin (hacking, mal- en ransomware), online geweld en cyberpesten. Dat geldt zelfs voor phishing, waar opvallend veel wetenschappelijk onderzoek naar is gedaan.

↩ Terug naar de overzichtspagina van dit hoofdstuk

CONCLUSIES EN AANBEVELINGEN | 6/6

[AANBEVELINGEN SLACHTOFFERS VOOR PRAKTIJK]

- Gebruik de positief geëvalueerde interventies en ontwikkel deze verder;
- Neem ook kennis van wat *niet* werkt en pas dit aan;
- Zet in op de gesignaleerde kansen voor interventies uit de praktijk en verzamelde inzichten uit de wetenschap;
- Ontwikkel integrale slachtofferhulp in publiek-private samenwerking;
- Ontwikkel en evalueer interventies op specifieke online criminaliteitsvormen voor senioren en jongeren;
- Ontwikkel en evalueer interventies ter preventie van slachtofferschap van cybercrime in enge zin, online geweld en cyberpesten;
- Maak gebruik van de rijke, wetenschappelijke inzichten rond slachtofferschap van online delicten als phishing.

[VERVOLGONDERZOEK SLACHTOFFERS]

- Breng op gestructureerde wijze de los gepubliceerde inzichten rondom slachtofferschap samen in scoping reviews en/of gestructureerde literatuurstudies;
- Ontwerp op basis van wetenschappelijke inzichten nieuwe interventies ter preventie van slachtofferschap samen met professionals uit publieke en private organisaties en evalueer deze op effect.

↩ Terug naar de overzichtspagina van dit hoofdstuk

SAXION UNIVERSITY OF APPLIED SCIENCES

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

CYBER WEERBAAR NL





CONTACT

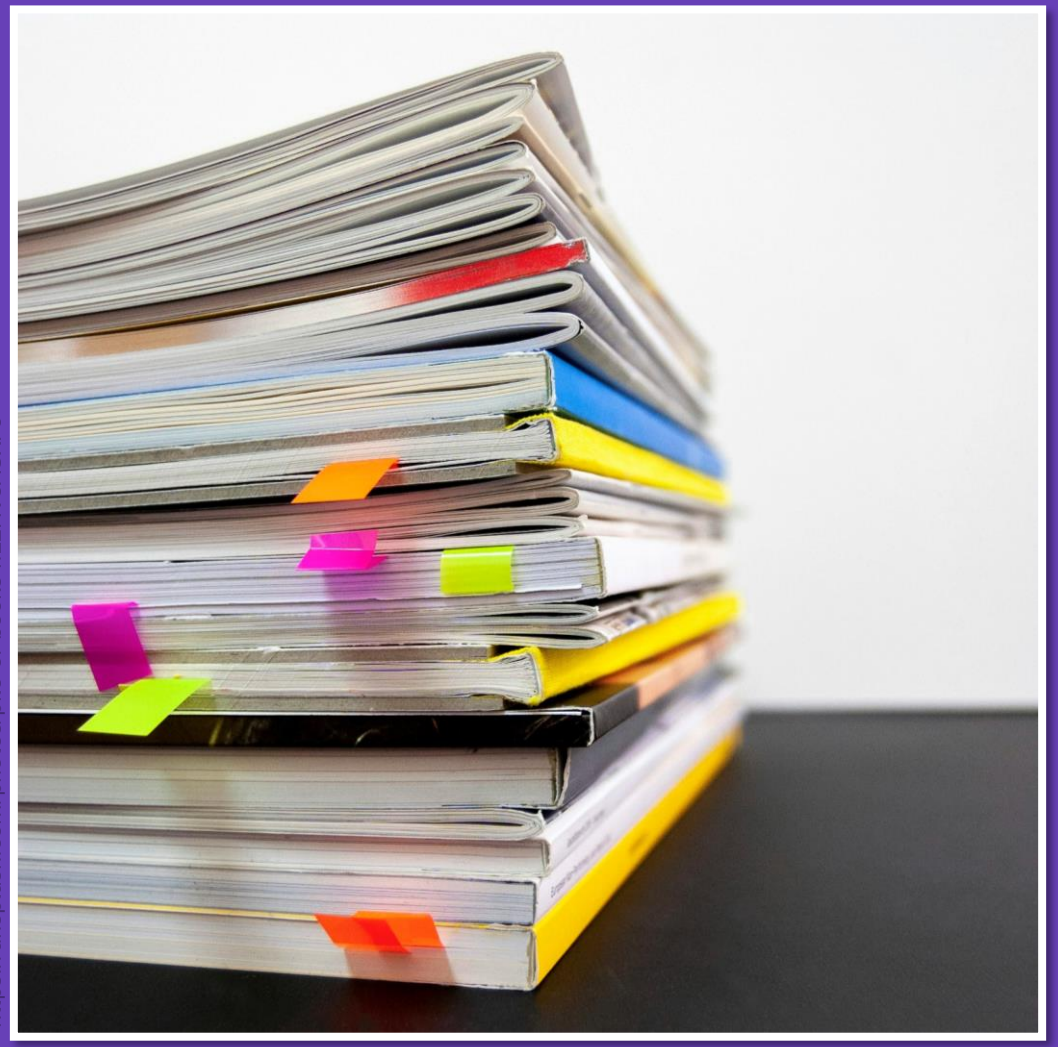
Thijs van Beek MSc., onderzoeker lectoraat Online Weerbaarheid, Hogeschool Saxion – o.m.j.vanbeek@saxion.nl

Elmira Land BA, onderzoeker lectoraat Online Weerbaarheid, Hogeschool Saxion – e.land@saxion.nl

Joeri Loggen MSC., onderzoeker lectoraat Cybercrime & Cybersecurity, de Haagse Hogeschool – j.loggen@hhs.nl

dr. Remco Spithoven, lector Online Weerbaarheid, Hogeschool Saxion – r.spithoven@saxion.nl

Prof.dr. Rutger Leukfeldt, lector Cybercrime & Cybersecurity, de Haagse Hogeschool - e.r.leukfeldt@hhs.nl



Afbeelding: Unsplash. (2019, 27 mei). https://unsplash.com/photos/pile-of-books-nE2HV5AUXFo

BIJLAGEN

OPBOUW

BIJLAGEN	
Bijlage 1:	**Inzichten uit de praktijk** Per delictsvorm
Bijlage 2:	**Scoping review daderschap** Resultaten per delictsvorm
Bijlage 3:	**Beschikbare interventies** Per delictsvorm en evaluatiestatus

ⓘ Klik op de onderstreepte bijlagen om naar de betreffende dia's te gaan

↩ Terug naar de inhoudsopgave

Afbeelding: eigen bezit, gemaakt tijdens kennissessie met praktijkpartners op 24 april 2024

BIJLAGE 1

Inzichten uit de praktijk: dader- en slachtofferschap online criminaliteit

OPBOUW BIJLAGE

BIJLAGE 1: INZICHTEN UIT DE PRAKTIJK

Bijlage 1.1: Daderschap

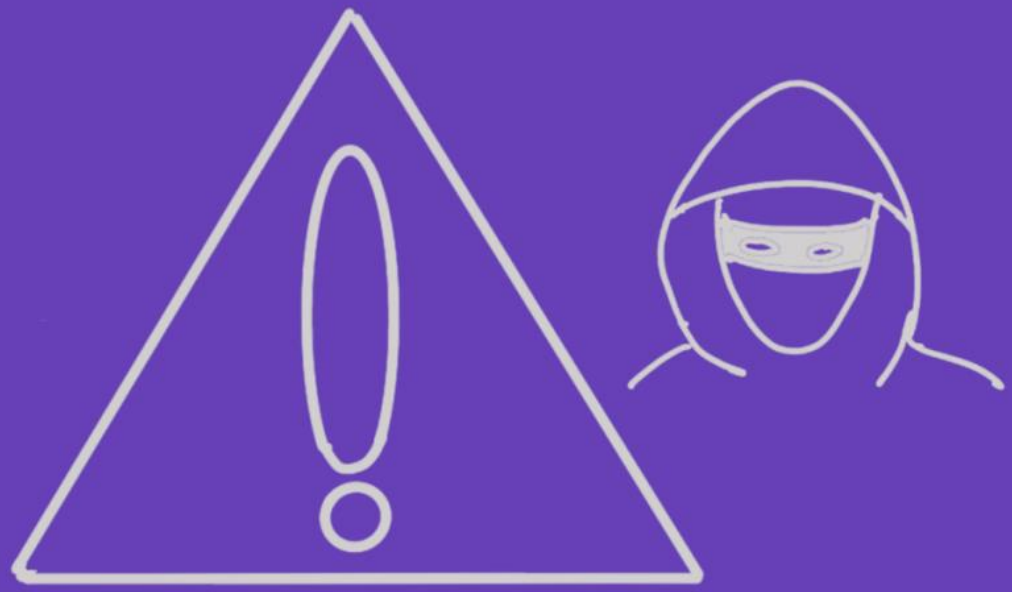
- Bijlage 1.1.1: Online criminaliteit, overkoepelend
- Bijlage 1.1.2: Cybercrime in enge zin
- Bijlage 1.1.3: Cyberstalking
- Bijlage 1.1.4: Malware
- Bijlage 1.1.5: Strafbare vormen van sexting
- Bijlage 1.1.6: Hacking
- Bijlage 1.1.7: Online fraude

Bijlage 1.2: Slachtofferschap

- Bijlage 1.2.1: Online criminaliteit, overkoepelend
- Bijlage 1.2.2: Online fraude
- Bijlage 1.2.3: Datingfraude
- Bijlage 1.2.4: Phishing

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

↩ Terug naar de inhoudsopgave



BIJLAGE 1.1

Inzichten uit de praktijk: daderschap online criminaliteit

Letterlijk uit de feedback overgenomen overzichten per delictstype

BIJLAGE 1.1.1: INZICHTEN UIT DE PRAKTIJK

DADERSCHAP | Online criminaliteit, overkoepelend

DADERS | Online criminaliteit, overkoepelend

INZICHTEN PRAKTIJKSESSIE | DADERSCHAP | ONLINE CRIMINALITEIT, OVERKOEPELEND			
Wat wordt herkend en wat mist er nog?	**Wat betekent dit in het voorkomen van daderschap?**	**Beleidsstukken, analyses of andere bronnen?**	**Good practices uit binnen- en buitenland (+ linkjes)**
▪ Geslacht? Leeftijd? ▪ Onderscheid tussen cybercrime en gedigitaliseerde criminaliteit ▪ Info over relatie qua criminele carrière en qua ‘crimineel werkveld’ tussen online criminaliteit, vormen van ondermijnende/georganiseerde criminaliteit ▪ Nog meer focus op daderschap veel voorkomende online criminaliteit, dat is nu heel actueel!	▪ Via politieonderzoek naar daders -> school identificeren -> weerbaarheidsinstructie inzetten ▪ Gericht onderzoek naar de plaatsen op internet waar 'social learning' plaatsvindt en dan offline halen ▪ Privaatrechtelijk aansprakelijk stellen, stopgesprek ed. ▪ Zie aanpak COPS, voor deze doelgroep ▪ Moeilijk zonder onderscheid 'high tech' vs 'low tech’ ▪ Social media (bv snapchat ads) inzetten om mensen met deze kenmerken te targetten	▪ Nee, alle onderzoek is heel pril. ▪ Fenomeenbeeld analyse 2024 ▪ Google Ads	▪ Nee, wel actief op zoek bilateraal naar EU-partners ▪ COPS

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.1.2: INZICHTEN UIT DE PRAKTIJK

DADERSCHAP | Cybercrime in enge zin | 1/2

INZICHTEN PRAKTIJKSESSIE | DADERSCHAP | CYBERCRIME IN ENGE ZIN
Wat wordt herkend en wat mist er nog?
▪ Slechte rolmodellen in wijk. We zien hotspots in grote steden; hoe kan dat? ▪ Verwachting was dat geslacht ook invloed zou hebben ▪ Sociale relaties, dat dat de negatieve relatie ten goede komt ▪ Rol van sociale media ▪ Statelijke actoren? ▪ Gaming ▪ Beperkt toezicht van ouders ▪ Leeftijd (deels) ▪ Gaming -> volgens onderzoek Haagse Hogeschool juist beschermend ▪ Uit de wetenschappelijke literatuur komt er naar voren dat het onduidelijk welk geslacht een verhoogde kans heeft op daderschap van cybercrime in enge zin, terwijl uit politie data voornamelijk mannen betreft ▪ Wat verder opvalt is dat bij andere (traditionele) vormen van criminaliteit jongeren vaker betrokken zijn en naarmate ze ouder worden dit afneemt. Bij cybercrime in enge zin zie je dit beeld niet terugkomen ▪ Belangrijk voor vervolgonderzoek: komen de onderzoeksresultaten overeen met de politie cijfers ▪ Daarnaast is het belangrijk om in het vervolgonderzoek duidelijk te definiëren wat criminaliteit in enge zin is en welke vormen van criminaliteit daaronder vallen ▪ De hoofddader moet *savy* zijn. Dus vaak zie je dat ze gamen of op andere wijze IT-kennis hebben, de bellers hebben vaak bij callcenters gewerkt want hun gesprekstechnieken zijn hetzelfde ▪ Iemand in de keten moet bepaalde kennis van de spullen hebben, maar deze technische kennis wordt ook gedeeld via kanalen als Telegram.

1/2

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.1.2: INZICHTEN UIT DE PRAKTIJK

DADERSCHAP | Cybercrime in enge zin | 2/2

INZICHTEN PRAKTIJKSESSIE | DADERSCHAP | CYBERCRIMINE IN ENGE ZIN		
Wat betekent dit in het voorkomen van daderschap?	**Beleidsstukken, analyses of andere bronnen?**	**Good practices uit binnen- en buitenland (+ linkjes)**
▪ Motivatie financieel, meer afpakken, status wegnemen ▪ Sociale relaties verbeteren/sociale cohesie ▪ Positief belonen en kennis/vaardigheden binden aan goede kant ▪ Meer aandacht voor/zicht op technische capaciteit van daders/jongeren ▪ Pakkans perceptie en impact van gepakt worden vergroten ▪ Koppeling zorg + IT ▪ Hoe verbinding leggen? Bv via games ▪ Voorlichting al starten op basisschool ▪ Combinatie gaming ASS, preventie maar breed regelen, bijz.onderwijs bv hulpverlening ▪ Technisch dichtzetten wat in de Modus Operandi nodig is, naam van de bank, sms ID en telefoonnummer van banken zijn intussen beschermd dus daar kan men zich niet meer voor uitgeven ▪ Geautomatiseerd signaleren van afwijkend verkeer en gedrag en daarop acteren ▪ Faciliterende organisaties en actoren mee gaan samenwerken en via pilots uitzoeken hoe je de M.O. kan verstoren en dat opschalen.	▪ COPS-THTL bronnen ▪ CCV aanpak daders cybercrime ▪ CSBN, NLCS, CCV integrale aanpak cybercrime ▪ Cahier Politiestudies 2020 -15 aard en omvang van dader- en slachtofferschap ▪ WODC ▪ Verwachte publicatie politie/OM;' cybercrimebeeld NL'	▪ Info uitwisselen, denk aan project Melissa ▪ COPS (2x) ▪ Voorbeelden van (inter)nationale onderzoeken ▪ Junior IOT ▪ Cyberbrein ▪ Mijn Cyberrijbewijs ▪ HackShield ▪ Rebootcamp ▪ Framed ▪ iSpoof en andere platformen uit de lucht halen ▪ Samenwerking is altijd de sleutel, iedereen heeft een deel van de oplossing in handen. Daarbij is het delen van kennis en informatie noodzakelijk.

2/2

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.1.3: INZICHTEN UIT DE PRAKTIJK

DADERSCHAP | Cyberstalking

INZICHTEN PRAKTIJKSESSIE | DADERSCHAP | CYBERSTALKING			
Wat wordt herkend en wat mist er nog?	**Wat betekent dit in het voorkomen van daderschap?**	**Beleidsstukken, analyses of andere bronnen?**	**Good practices uit binnen- en buitenland**
▪ Buitengesloten/geen onderdeel van de samenleving ▪ Veel LVB achtergrond ▪ Online cyberstalking, herkenning ▪ Deviante vrienden, middelengebruik ▪ Relatie tussen dader-SO? ▪ Concretisering m.b.v. voorbeelden van abstracte begrippen zoals etniciteit en persoonlijkheidskenmerken? ▪ Ik herken autisme, aangetroffen bij puber die aan sextortion deed ▪ Bijna alles wat is genoemd	▪ Strafrechtelijke handhaving op dit gebied zorgt waarschijnlijk niet voor het voorkomen/verstoren -> niet strafrechtelijke interventies werken waarschijnlijk beter ▪ Online gebiedsverbod ▪ Combi van factoren = profiel? Witte mannen eerder slachtoffer psychische problemen bijvoorbeeld?	-	-

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.1.4: INZICHTEN UIT DE PRAKTIJK

DADERSCHAP | Malware

INZICHTEN PRAKTIJKSESSIE | DADERSCHAP | MALWARE			
Wat wordt herkend en wat mist er nog?	**Wat betekent dit in het voorkomen van daderschap?**	**Beleidsstukken, analyses of andere bronnen?**	**Good practices uit binnen- en buitenland**
▪ Negatieve relaties mbt vormen van toezicht? ▪ Competentiedrang tussen daders: 'laten zien welke skills je hebt'? ▪ Financieel motief	▪ Neutraliseren van neutralisatie technieken ▪ Pakkans perceptie+impact van gepakt worden vergroten ▪ Toezicht (zorg/sociaal) in stelling brengen ▪ 'Vroegsignalering' noodzakelijk bij risicogroepen via scholen, jeugd, ggz, hackerplatformen etc ▪ Maatschappelijke stage IT bedrijf	▪ Analyse politiedossiers (to be done?)	▪ Infiltratie hackfora

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.1.5: INZICHTEN UIT DE PRAKTIJK

DADERSCHAP | Strafbare vormen van sexting

INZICHTEN PRAKTIJKSESSIE | DADERSCHAP | STRAFBARE VORMEN VAN SEXTING			
Wat wordt herkend en wat mist er nog?	**Wat betekent dit in het voorkomen van daderschap?**	**Beleidsstukken, analyses of andere bronnen? (+ link)**	**Good practices uit binnen- en buitenland (+ link)**
▪ Relatie tot SO ▪ SO eerder SO in soortgelijke incidenten ▪ Narcistisch, empathie dader ▪ De relatie die de daders hebben tot vrouwen/het denkbeeld over vrouwen? ▪ Autisme-> zorg inrichten op voorlichting online fatsoensnormen ▪ Groepsdruk; als sextortion genormaliseerd is, dan is de groepsdruk juist om door te gaan ▪ (Intuïtief) mogelijk mist iets als eigen drive op seksueel vlak ▪ Factor macht/controle?	▪ Toezicht vanuit ouders ▪ Lessen over impact (tot zelfdoding aan toe!) ▪ Over sexting wordt gezegd dat het niet meer weg zal gaan ▪ Uitleg aan jongeren over ongecontroleerde verspreiding op internet ▪ Vorming via invloed ouder of onderwijs noodzakelijk ▪ Privaatrechtelijk aansprakelijk stellen	▪ Fenomeenbeeld analyse 2024 ▪ Dossiers sextortion Politie Oost NL	▪ Project Shitzooi (Katwijk)

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.1.6: INZICHTEN UIT DE PRAKTIJK

DADERSCHAP | Hacking

INZICHTEN PRAKTIJKSESSIE | DADERSCHAP | HACKING			
Wat wordt herkend en wat mist er nog?	**Wat betekent dit in het voorkomen van daderschap?**	**Beleidsstukken, analyses of andere bronnen? (+ linkjes)**	**Good practices uit binnen- en buitenland (+ linkjes)**
▪ De link met traditionele criminaliteit; denk aan (vuur)wapens? ▪ Ouderlijk toezicht herkenbaar ▪ Negatieve relatie m.b.t. andere vormen van toezicht (school, jongerenwerk etc.) ▪ 'Gedigitaliseerde criminaliteit/online fraude? ▪ Reden voor eenvoudige hacking: denk aan ex-hackt-ex? ▪ 'Werk in IT' ook risicofactor? ▪ Herkenbaar	▪ Sociaal economische status ▪ Omgeving beïnvloeden ▪ Pakkans perceptie + impact van gepakt worden vergroten ▪ Richten op preventieve aanpak (aangezien negatieve rol icm ouderlijk toezicht) helemaal aangezien deviante vrienden ook benoemd wordt als positieve relatie ▪ Inzoomen op SES+neutralisatietechnieken in de preventieve aanpak ▪ Relatie delict/leed leggen ▪ Statussymbolen afpakken ▪ Daderpreventie richten op mensen met dit type kenmerken ▪ Moraliteit beïnvloeden in onderwijs door confrontatie met slachtoffer verhalen ▪ Hoe inzetten rol ouders/docenten?	▪ Politiedata (kenmerken verdachten, criminele carrières) ▪ Interviews met hackers? Weet niet of deze er zijn ▪ CBS ▪ Cyberbeelden/politie ▪ Fraudehelpdesk ▪ Slachtofferhulp ▪ Veiligheidsmonitor	▪ Zie ook input bij cybercrime in enge zin ▪ Betaalaccounts beter beveiligen ▪ Consumenten inlichten over hacken ▪ Hackright ▪ Interventie hackfora gebruikers/ darkmarkets ▪ Correctiemechanisme onder hackers ('Viktor Gevers') ▪ Vraag het COPS ▪ Deter, divert, degrade, disrupt ▪ COPS ▪ Re-bootcamp

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.1.7: INZICHTEN UIT DE PRAKTIJK

DADERSCHAP | Online fraude | 1/2

INZICHTEN PRAKTIJKSESSIE | DADERSCHAP | ONLINE FRAUDE	
Wat wordt herkend en wat mist er nog?	
Positieve factoren ▪ Digitale kennis ▪ Confrontatie met F-game op social media; zou makkelijk zijn, veel geld verdienen ▪ Slechte financiële positie/strain ▪ Deviante vrienden ook traditionale netwerkjes ▪ ‘Gedwongen' criminele carrière na eerste stappen als bv geldezel ▪ Webinar LVB professionals ▪ Social engineering ▪ ‘Cultuur' oa dure kleding en auto’s ▪ Verwevenheid traditionele criminaliteit ▪ Verplaatsing darkweb -> oa Telegram ▪ Status van de straat! Sociale media ▪ LVB en junks geldezels en katvangers ▪ Idolen bv influencers	**Negatieve factoren** ▪ Beïnvloedbare jongeren: leeftijdsfase, ontwikkeling hersenen, impuls onderdrukking ▪ Leeftijd, opleidingsniveau, toezicht ouders ▪ Online HIC=offline HIC (dadergroepen) ▪ Idolen bv influencers ▪ Lage pakkans

1/2

BIJLAGE 1.1.7: INZICHTEN UIT DE PRAKTIJK

DADERSCHAP | Online fraude | 2/2

INZICHTEN PRAKTIJKSESSIE | DADERSCHAP | ONLINE FRAUDE		
Wat betekent dit in het voorkomen van daderschap?	**Beleidsstukken, analyses of andere bronnen? (+ linkjes)**	**Good practices uit binnen- en buitenland (+ linkjes)**
-	▪ CBS ▪ Fenomeenbeeld analyse 2024 ▪ Onderzoek civiele aansprakelijkstelling hhs ▪ Politiedata verdachten ▪ Veiligheidsmonitor (2x) ▪ Politiedata ▪ Pathways	▪ Verbinding met traditionele criminaliteit, bv f-game ▪ Uitwerken 'criminal journeys' als basis voor uitwerken barrièremodellen om interventies te ontwikkelen ▪ Directe aansprakelijkheid pilots ▪ Samenwerking ▪ COPS methodiek ▪ Integrale aanpak online fraude ▪ Gedragsbeïnvloeding online via advertenties en doorgeleiding ▪ Wasstraat geldezels ▪ Delen onderzoeksresultaten ▪ Preventie ▪ Top 60

2/2

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.2

Inzichten uit de praktijk: slachtofferschap online criminaliteit

Letterlijk uit de feedback overgenomen overzichten per delictstype

BIJLAGE 1.2.1: INZICHTEN UIT DE PRAKTIJK

SLACHTOFFERSCHAP | Online criminaliteit, overkoepelend | 1/2

INZICHTEN PRAKTIJKSESSIE | SLACHTOFFERSCHAP | ONLINE CRIMINALITEIT, OVERKOEPELEND
Wat wordt herkend en wat mist er nog?
- Herkenbaar - Verbazing: waarom zijn vrouwen meer slachtoffer? - Geslacht (vrouw) is te kort door de bocht en verschilt per delict! - Vrouwen worden meer slachtoffer van datingfraude niet van aan/verkoopfraude bijvoorbeeld - Leeftijd verschilt ook sterk per delict bijvoorbeeld sextortion (jong) en bankhelpdeskfraude (oud) - Hoe passen geldezels in dit beeld? Is dit dader- of slachtofferschap? - Zijn slachtoffers ook "extra" kapitaal krachtig? - Cyberschaamte? - Ik herken de gevoeligheid voor autoriteit heel erg. - "Brave" omgeving, zoals een dorpje - Ambiguiteit: er is een duidelijk onderscheid in leeftijd/geslacht tussen verschillende vormen van online fraude - IT skills moeten ook naar ambigu - Algemene campagnes die werken met "Zonde van het geld“?

1/2

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.2.1: INZICHTEN UIT DE PRAKTIJK

SLACHTOFFERSCHAP | Online criminaliteit, overkoepelend | 2/2

INZICHTEN PRAKTIJKSESSIE | SLACHTOFFERSCHAP | ONLINE CRIMINALITEIT, OVERKOEPELEND		
Wat betekent dit in het voorkomen van daderschap?	**Beleidsstukken, analyses of andere bronnen? (+ linkjes)**	**Good practices uit binnen- en buitenland (+ linkjes)**
- Lage computerkennis - Ander profiel bij de bank, eerdere detectie - Bij bankhelpdeskfraude heeft het slachtoffer na ophangen direct door dat het niet klopt, tijdens gesprek ook al onbehagen - Modus Operandi verstoren - Gelegenheidsstructuren verstoren - Cyberschaamte doorbreken - Meldingsbereidheid vergroten - Preventie én nazorg - Ervaringsverhalen delen - Koppeling tussen hulp, nazorg en preventie z.s.m. bij melding (waar dan ook) om herhaald slachtofferschap te voorkomen - Identificeren van plaatsen voor b.v. datingfraude en daar detectie en preventiemaatregelen op zetten - Slachtofferschap nabootsen - Voorkomen van delict (verstoren) heeft meer impact dan voorkomen door voorlichting - Gespecialiseerd team voor online slachtofferpreventie	- 2x onderzoek cyberschaamte politie Rotterdam, cyber en communicatie - Onderzoek meldingsbereidheid van slachtoffers van Ransomware in de haven van Rotterdam - Microdata CBS - Onderzoeken GASA - Onderzoek UT Fraude victimisatie - Fenomeenbeeld '24 Politie - Onderzoek Jildau Borwell - Check cyberbeelden politie voor delicten vs. Leeftijd - Onderzoek consumentenbond '23	- Scam survivors – UK - Whatsnep - Echt nep - Rotterdam (interactieve film) 2x 2/2

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.2.2: INZICHTEN UIT DE PRAKTIJK

SLACHTOFFERSCHAP | Online fraude

INZICHTEN PRAKTIJKSESSIE | SLACHTOFFERSCHAP | ONLINE FRAUDE			
Wat wordt herkend en wat mist er nog?	**Wat betekent dit in het voorkomen van daderschap?**	**Beleidsstukken, analyses of andere bronnen?**	**Good practices uit binnen- en buitenland (+ linkjes)**
▪ De vaardigheden t.a.v. digitale veiligheid moeten naar de categorie negatieve relatie, dat is logischer ▪ Relatie tot vermogen. Ouderen hebben doorgaans hun financiele huishouding op orde. ▪ Herkenbaar ▪ Social engineering mist ▪ Goedgeloving/naief zijn mist ▪ Mentale aspect: gevoelig zijn voor druk. ▪ Routine activiteiten: Jongeren veel en oppervlakkig, ouderen minder en argeloos ▪ Schaamte ▪ Kwetsbaarheid ▪ Leeftijd? Van bankhelpdeskfraude en hulpvraagfraude worden vooral ouderen het slachtoffer ▪ Zelfcontrole bij negatieve relaties? ▪ Schaamte/stigma is een riscofactor voor slachtofferschap/impact? ▪ Eerder slachtofferschap als risicofactor ▪ Uitsplitsen voor veelvoorkomende vormen als hulpvraagfraude, bankhelpdeskfraude, aankoopfraude, e.d.	▪ Cyberschaamte doorbreken ▪ Ook hier: maak een slachtoffer journey als basis voor interventies ▪ Handelingskader per type delict.	▪ Criminal journey in kaart gebracht bankhelpdesk-fraude ▪ De schaamte die slachtoffers ervaren van digitale fraude onderzoek	▪ Betrekken van naasten in de preventie. Vooral bij ouderen de (klein)kinderen ▪ Bereik ze via hun kanalen (contacten)! ▪ Campagne 'Frauderen zo werkt het' ▪ Check je belletje/ telefoontje van de bank in de app checken (ING pilot)

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.2.3: INZICHTEN UIT DE PRAKTIJK

SLACHTOFFERSCHAP | Datingfraude

INZICHTEN PRAKTIJKSESSIE | SLACHTOFFERSCHAP | DATINGFRAUDE			
Wat wordt herkend en wat mist er nog?	**Wat betekent dit in het voorkomen van daderschap?**	**Beleidsstukken, analyses of andere bronnen? (+ linkjes)**	**Good practices uit binnen- en buitenland (+ linkjes)**
▪ Eenzaamheid/isolement ▪ Herkenning ▪ Schaamte aspect mist ▪ Sociaal netwerk? ▪ Eenzaamheid, zelfisolatie en *social engineering*? ▪ Ouderen meer plichtsgetrouw ▪ Had verwacht dat geslacht (vrouw) bij ambigue stond ▪ Eenzaamheid	▪ Al op de dating site (red flags) op foto? ▪ Samenwerking met sociale media bedrijven ▪ Sneller actuele MO's delen met breed publiek ▪ Interventies richten op verstoren van gelegenheidsstructuur ▪ Sociaal vangnet creëren voor slachtoffers ▪ Veel goede aanknopingspunten voor interventies per doelgroep ▪ Psychologen vragen om interventies te ontwikkelen ▪ Slachtoffers blijven geloven, ook als fraude hard aangetoond is! ▪ Barrières in datingapps en ID-functie facebook e.d.	▪ FBI cyberbeeld ▪ Chainanalysis jaarbeeld (aard en omvang) ▪ Fraudehelpdesk	▪ Operation shamrock US ▪ Operation level up US ▪ (Pigbutchering slachtoffers) ▪ 4 uur voordat je limiet gewijzigd is bij bankrekening zodat de hoop is dat men erover nadenkt ▪ Scène uit film echt of nep? VAR

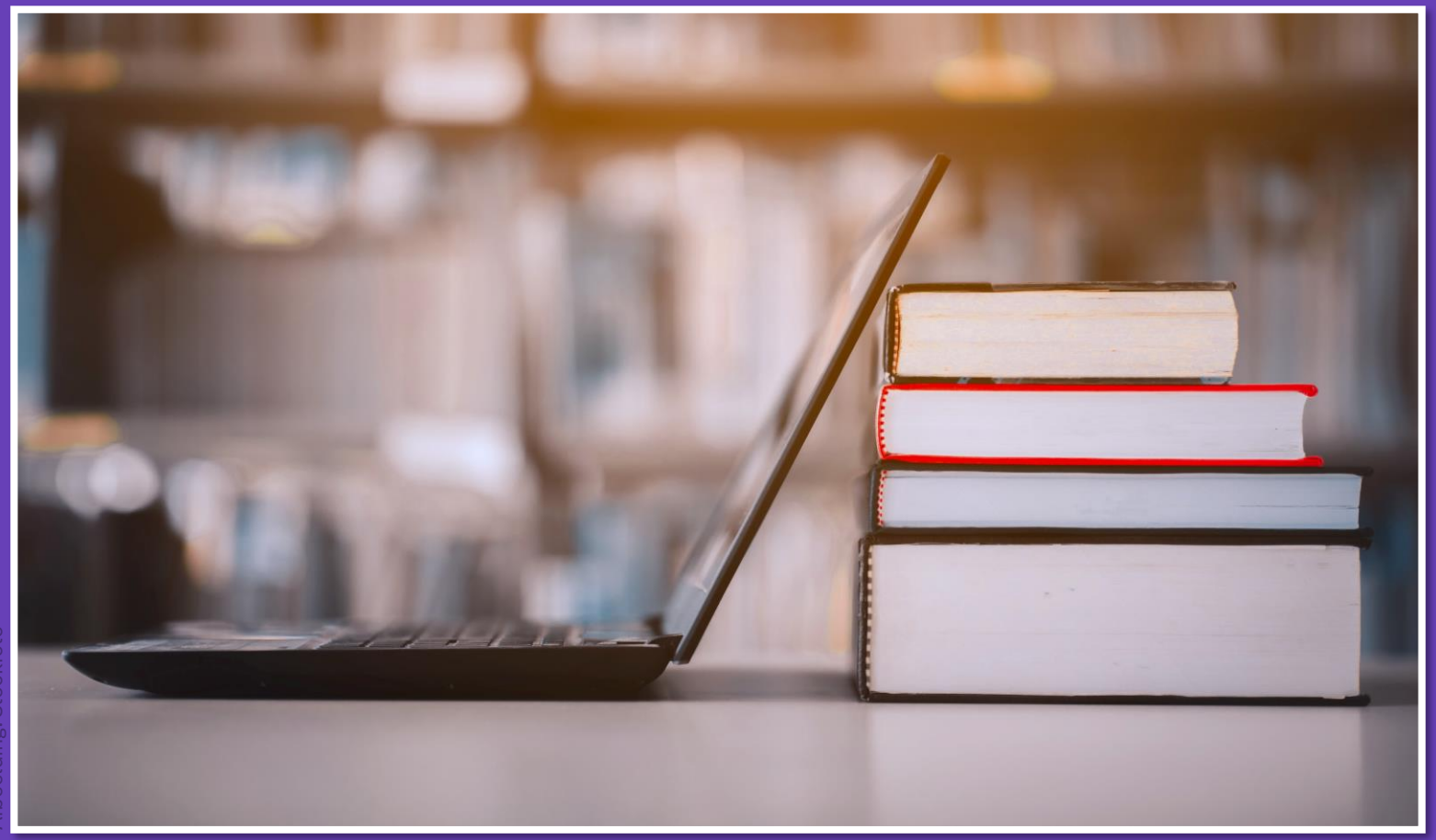
↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 1.2.4: INZICHTEN UIT DE PRAKTIJK

SLACHTOFFERSCHAP | Phishing

INZICHTEN PRAKTIJKSESSIE | SLACHTOFFERSCHAP | PHISHING			
Wat wordt herkend en wat mist er nog?	**Wat betekent dit in het voorkomen van daderschap?**	**Beleidsstukken, analyses of andere bronnen?**	**Good practices uit binnen- en buitenland**
▪ Particulieren vs. bedrijven; beter uitsplitsen ▪ Uit naam instantie (belasting, politie etc); herkenning ▪ Schaamte ▪ In relatie tot andere criminaliteit bv als start van ransomware	▪ Fake phishingsmails ▪ Slachtoffernotificatie na datalek-/hack ▪ Meer gerichte training/inverventie-programma's op basis van dat onderzoek ▪ 'Tooling': go-go look, DNS? Alertmelding verdachte sms/mail	▪ Onderzoek cyberschaamte bij phishing; Britt Weteling	▪ Preventie

↩ Terug naar de overzichtspagina van deze bijlage



Afbeelding: Stockfoto

BIJLAGE 2

Inzichten op gebied van daderschap uit de scoping review

OPBOUW BIJLAGE

BIJLAGE 2: INZICHTEN OP GEBIED VAN DADERSCHAP UIT DE SCOPING REVIEW	
Vooraf: legenda	
Bijlage 2.1: Hacking Bijlage 2.2: Malware Bijlage 2.3: Online fraude Bijlage 2.4: Phishing Bijlage 2.5: Vishing Bijlage 2.6: Datingfraude Bijlage 2.7: Pig-butchering scam Bijlage 2.8: Advance fee fraud Bijlage 2.9: E-commerce fraude	Bijlage 2.10: Concession-Abuse-as-a-Service (CAaaS)-fraude Bijlage 2.11: Online werkgelegenheidsfraude Bijlage 2.12: Online werknemersfraude Bijlage 2.13: Online bankpasfraude Bijlage 2.14: Social engineering Bijlage 2.15: Geldezels Bijlage 2.16: Bitcoin-gerelateerde online criminaliteit Bijlage 2.17: Overig

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

↩ Terug naar de inhoudsopgave

LEGENDA

VOOR IEDERE GEKLEURDE CATEGORIE

VOOR IEDERE CATEGORIE BEHALVE TRENDS, TOEKOMSTIG ONDERZOEK, INTERVENTIES/TRAININGEN	
Groen tekstvak	**Positieve relatie**: hoe meer iemand dit kenmerk heeft of dit gedrag vertoont, hoe groter de kans dat hij of zij dader of slachtoffer wordt.
Rood tekstvak	**Negatieve relatie**: hoe meer iemand dit kenmerk heeft of dit gedrag vertoont, hoe kleiner de kans dat hij of zij dader of slachtoffer wordt.
Blauw tekstvak	**Ambigue relatie**: het is onduidelijk wat de invloed van dit kenmerk of dit gedrag is op dader- of slachtofferschap.

>> In verband met de omvang van de tabellen, worden de legenda's voor deze bijlage enkel op deze en volgende dia weergegeven.

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

↩ Terug naar de overzichtspagina van deze bijlage ↩ Terug naar paragraaf 3.3

LEGENDA

VOOR TRENDS, TOEKOMSTIG ONDERZOEK EN INTERVENTIES/TRAININGEN

VOOR DE CATEGORIEËN TRENDS, TOEKOMSTIG ONDERZOEK, INTERVENTIES/TRAININGEN	
Opsommingsteken +	**Opkomend/aanbeveling**: (1) trends die opkomend, in veranderding of in ontwikkeling zijn, (2) aanbevelingen voor meer toekomstig onderzoek (3), interventies/ trainingen waar vanuit de focus op moet komen te liggen.
Opsommingsteken –	**Niet opkomend/geen aanbeveling:** (1) trends die niet opkomend, in veranderding of in ontwikkeling zijn, (2) geen aanbevelingen voor meer toekomstig onderzoek (3), interventies/trainingen waar niet de focus op moet komen te liggen.
Opsommingsteken ±	**Onduidelijk:** (1) onduidelijk of trends die opkomend, in veranderding of in ontwikkeling zijn, (2) onduidelijk omtrent aanbevelingen voor meer toekomstig onderzoek (3), onduidelijk over interventies/trainingen waar de focus op moet komen te liggen.

>> In verband met de omvang van de tabellen, worden de legenda's voor deze bijlage enkel op deze dia weergegeven.

ⓘ Klik op de paragraaftitels om naar de betreffende dia’s te gaan

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.1: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Hacking

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/dader)
Geslacht en leeftijd	Strafblad en recidive	Chatrooms	Peers		Neutralisatie-technieken (algemeen)	Gebruikte kanalen	+ Frequentie	+ Chatrooms en sociale media	+ Monitoren
					Hogere morele principes	Koopbaarheid van persoonsgegevens	- Relatie tot het slachtoffer	+ Steekproef	+ Bewustzijn schade
					Ontkennen van slachtofferschap	Persoonlijke informatie			+ Neutralisatie-technieken
					Rechtvaardigingsclaim				± Afschrikking
					Veroordelaars veroordelen				
					Verspreiding van schuld				
					Persoonlijke rechtvaardiging				
					Ontkennen van schade				
					Persoonlijke rechtvaardiging				
					Rechtvaardiging door vergelijking				
					Rechtvaardiging o.b.v. noodzaak				
					Verantwoordelijkheid ontkennen				
					Game-items				
					Plezier en impulsiviteit				
					Woede				

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.2: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Malware

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macrofactoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
				Internetgebruikers		Blokkeren van toegang		+ Multilevel model	
				Welvaart		Social engineering			
						Verspreiding via download of bijlages in e-mails			

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.3: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Online fraude (algemeen)

DADERS | Online fraude (algemeen)

Demo-grafische kenmerken	Intrinsieke en persoonlijk-heids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/dader)
			Gedeelde banden en gemeen-schappelijke affiliaties	Internetgebruik	Neutralisatie bij ouders van fraudeurs	Anticiperen	+ Afwezigheid capabele bewaker	+ Effectiviteit van verlies-geframede waarschuwingen	+ Detectie en monitoren
			Groeps-interactie	Welvaart	Financieel gewin	Samenwerking corrupte overheids-functionarissen		+ Externe validiteit	+ Documenteren aard en omvang fraude
			Mentorschap		Hebzucht	Smurfen		+ Generaliseer-baarheid en diversiteit	+ Evaluatie maatregelen
			Ouders			Technologie		+ Kwetsbaarheid demografische groepen	+ Ondersteuning slachtoffers
						Verliesaversie		+ Longitudinaal onderzoek	+ Impact verkleinen bij slachtoffers
						Autoriteit		+ Modus operandi	+ Fraudebestrijdingsplan bij toekomstige crisis
						Schaarste		+ Rol medeplichtigen	+ Armoedebestrijding
						Urgentie		+ Timing en waarschuwings-berichten	+ Gezins- en sociale omgeving
									+ Strikte en onvermijdelijke straffen
									+ Aanpakken van neutralisaties en rationalisaties

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.4: INZICHTEN UIT DE SCOPING REVIEW

DADERS | Phishing

DADERSCHAP | Phishing

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
						Algemene termen in e-mails	+ Disproportioneel aandeel	+ Motivatie oplichter	+ Adequaat handelen
						Autoriteit	+ Frequentie	+ Sociale contexten	+ Bewustwording
						Behulpzaamheid		+ Sociale manipulatie	+ Detectie-methoden
						Decoy-pagina's		+ Vergelijkend onderzoek	+ Monitoren
						Dreiging			+ Phishingkits repository
						Levensduur phishing-aanval			+ Wetshandhaving
						Phishingkits			
						Sociale context			

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.5: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Vishing

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
					Financieel gewin	Interactie		+ Misdaadscripts	+ Bewustwording
						Rekrutering			+ Misdaadscripts
						VoIP-technologie			+ Samenwerking
						Autoriteit			
						Onder druk zetten			

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.6: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Datingfraude

Demo-grafische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/dader)
		Anonimiteit	Diaspora	Economische marginalisatie	Altercasting	Beloning	+ Frequentie	+ Blokkeren communicatie	+ Bewustzijn
		Betaalbaar-heid	Sociale banden	Patriarchale normen	Ontkennen van slachtofferschap	Opvolgberichten	+ Ondersteunende rol vrouw	+ Meldingsgedrag	+ Certificering van datingsites
						Gesprek voortzetten op een ander platform	- Nepaccounts identificeren	+ Menselijk gedrag	+ Detectie
						Passend profiel		+ Modus operandi	+ Empathieniveau
						Opvragen persoonlijke informatie		+ Psychologische kenmerken en gevolgen	+ Geestelijke gezondheid
						Inschakelen handlangers		+ Steekproef	+ Genderdiscours
						Platform			+ Heersende norm
						Vertrouwen opbouwen			+ Meldingspunt voor slachtoffers
						Begeerlijk			+ Monitoren
						Geloofwaardig			+ Risico-identificatie
						Gevoel van controle en zelfvertrouwen			+ Samenwerking
						Herhaaldelijke verzoeken			+ Screeningtools
						Persoonlijke verhalen			+ Victim-blaming voorkomen
						Religieuze band			+ Voorlichting
						Romantische band			+ Waarschuwingsberichten
						Toewijding			+ Zelfbeschermings-maatregelen
						Urgentie			+ Afschrikking
									+ Culturele normen veranderen
									+ Morele en juridische gevolgen

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.7: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Pig-butchering scam

DADERS | Pig-butchering scam

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macrofactoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
						Misleiding		+ Mixed method	+ Herstel en re-integratie
									+ Samenwerking

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.8: INZICHTEN UIT DE SCOPING REVIEW

DADERS | Advance fee fraud

DADERSCHAP | Advance fee fraud

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macrofactoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/dader)
				Politiek en economisch klimaat		Digitale omgeving	+ Normalisatie	+ Real-time data	+ Bewustwording
						Hybride interactie	+ Robin Hood	+ Social engineering-technieken	+ Attitudes
						Profiel	+ Zoekmachines	+ Verklaren dadergedrag	+ Maatschappelijke norm
						Social engineering			+ Rehabilitatie- en preventie-programma's
						Verhogen van eisen			+ Routine-activiteiten theorie
									+ Sancties
									+ Voorlichting

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.9: INZICHTEN UIT DE SCOPING REVIEW

DADERS | E-commerce fraude

DADERSCHAP | E-commerce fraude

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macrofactoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
Geslacht						Platforms		+ Meerdere landen	+ Bewustzijn
Leeftijd								+ Modus operandi	

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.10: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Concession-Abuse-as-a-Service (CAaaS)-fraude

DADERS	Concession-Abuse-as-a-Service (CAaaS)-fraude

Demo-grafische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/dader)
	Betrokkenheid bij niet-oplichters praktijken					Gecompromiteerde accounts	+ Tutorials en begeleiding forum		+ Account Abuse Detection Principles (AADP)
						Misbruik retourbeleid			+ Merchant Operation Protocol (MER-OP)
						Telefoongesprekken			
						Beleefdheid			
						Medelijden en urgentie			
						Liegen over eerdere gesprekken			
						Wettelijke voorschriften uitbuiten			

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.11: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Online werkgelegenheidsfraude

Demo-grafische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/dader)
						Autoriteit		+ Maatschappelijke impact	+ Onderwijs en bewustwording
						Beleefde toon		+ Psychologische mechanismen	+ Samenwerking
						E-mail		+ Verschillende demografie	+ Wetgeving
						Focus op niet-technologisch beroep			
						Gedrag aanpassen en imitatie			
						Schaarste			
						Sociale bewijskracht			
						Sociale nabijheid			
						Verliesaversie			
						SES en opleidingsniveau			

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.12: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Online werknemersfraude

Demo-grafische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/dader)
Geslacht en werkpositie	Ondeugd	Ongebruikelijk gedrag	Misbruik door familie		Rationalisaties	Salaris-tarieven manipuleren	+ Ongecontroleerde toegang	+ Meerdere landen	+ Audits
Leeftijd	Strafblad							+ Sector-vergelijking	+ Het vier-ogen-principe
									+ Verplichte vakanties en functiewisselingen
									+ Achtergrond-informatie werknemer
									+ Afschrikking

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.13: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Online bankpasfraude

Demo-grafische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/dader)
					Financieel gewin	Aankopen bankkaart-gegevens			+ Bewustwording
						Geldezels			+ Samenwerking
						Netwerk			+ Bewustwording
						Skimming			
						Software voor transacties			
						SQL-injectie			
						Verbergen identiteit			
						Vluchtgedrag			
						Directe interactie			

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.14: INZICHTEN UIT DE SCOPING REVIEW

DADERS | Social engineering

DADERSCHAP | Social engineering

Demo-grafische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
						Gedrag afstemmen		+ Demografische factoren	
						Normaal overkomen		+ Modus operandi en detectie-mechanismen	
						Overtuigend profiel		+ Motivatie	
						Realistisch scenario schetsen		+ Psychologische en sociale mechanismen van slachtoffers	
						Snel en eenvoudig			
						Sociale norm			
						Timing			
						Authenticiteit			
						Autoriteit			
						Beloning en behulpzaam zijn			
						Urgentie en druk			

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.15: INZICHTEN UIT DE SCOPING REVIEW

DADERS | Geldezels

DADERSCHAP | Geldezels

Demo-grafische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
						Financieel	+ Subcultuur		+ Bewustwording
						Gesloten netwerken			+ Peer pressure en subculturele normen
						Neutralisatie- en normalisatie-technieken			+ Voorlichting
						Instagram			+ Accounts blokkeren
						Presenteren als reguliere bedrijven			+ Anonimiteit verminderen
						Privé-chats			+ Monitoren en waarschuwingen
						Regionale gerichtheid			

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.16: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Bitcoin gerelateerde online criminaliteit

DADERS	Bitcoin gerelateerde online criminaliteit

Demo-grafische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
							+ Concentratie criminaliteit		+ Bewustwording
									+ Detectie

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.17: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Overig 1/4 | Computergerelateerde cybercriminaliteit

DADERS	Overig: computer-gerelateerde cyber-criminaliteit

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
Geslacht (man)	Recidive				Financieel gewin	E-mail en mobile messenger	+ Bewustzijn		+ Authenticatie- en registratiesystemen
Leeftijd	Strafblad					Impersonatie	+ Gemakkelijke toegang tot persoonsgegevens		+ Gebruikersidentificatie en notificatie-functies
									+ Regulering en aansprakelijkheid

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.17: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Overig 2/4 | Contentgerelateerde cybercrime

DADERS	Overig: content-gerelateerde cyber-criminaliteit

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
Geslacht (man)	Strafblad				Persoonlijke veroordeling	Anonimiteit	+ Gemakkelijke toegang tot persoonsgegevens		+ Beheersysteem
Burgerlijke staat	Recidive				Plezier en verveling	Contact via berichten of telefonisch	+ Relatie tot het slachtoffer		+ Detectie
Leeftijd					Slechte ervaringen	Publieke verspreiding			+ Gebruikerscontrole
					Solidariteit met pestkop				+ Schadelijke inhoud brokkeren
					Woede				

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 2.17: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Overig 3/4 | Witwassen

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
						Geldezels			

↩ Terug naar de overzichtspagina van deze bijlage

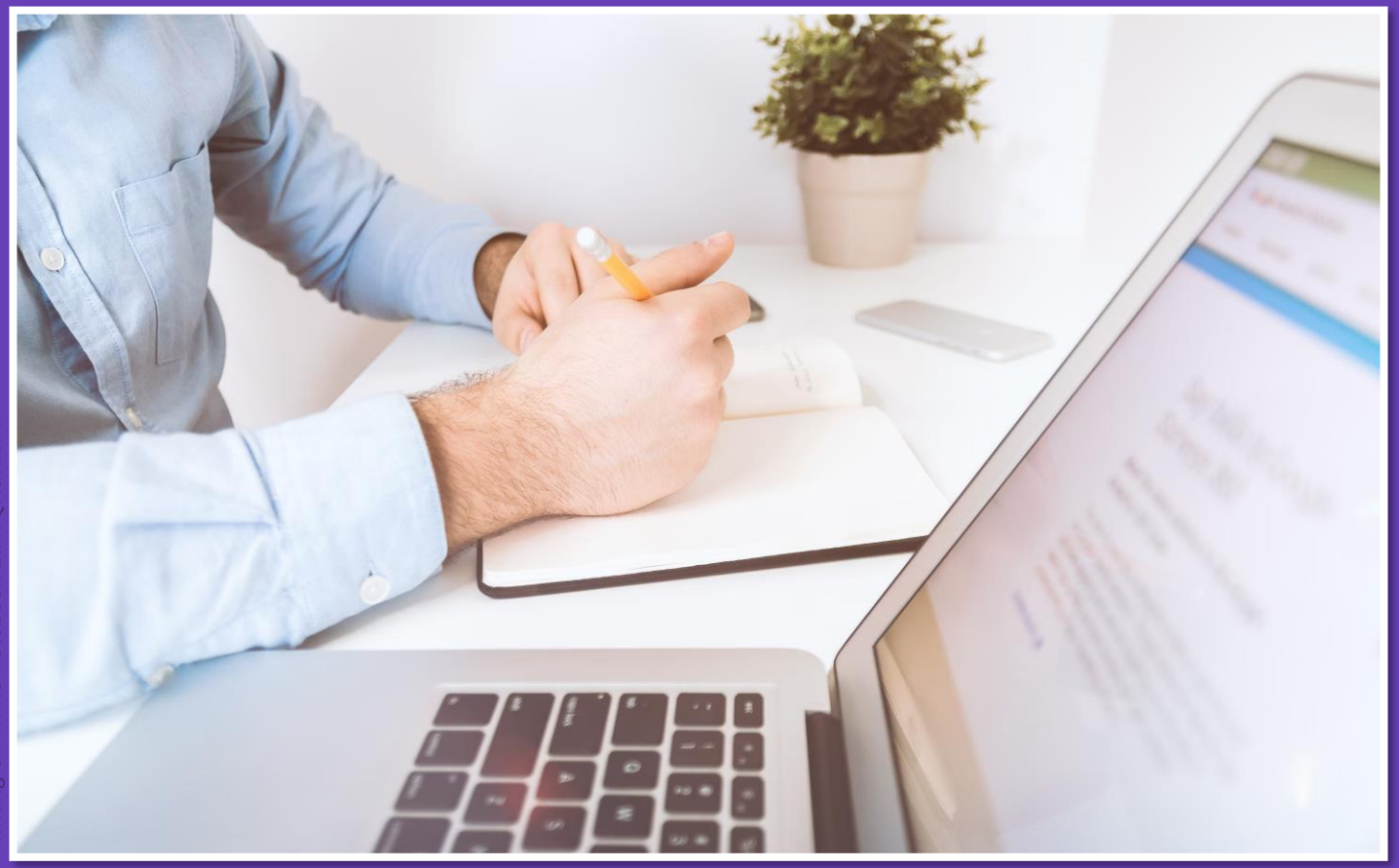
BIJLAGE 2.17: INZICHTEN UIT DE SCOPING REVIEW

DADERSCHAP | Overig 4/4 | Business Email Compromise (BEC)-fraude

DADERS	Overig: Business Email Compromise (BEC)-fraude

Demografische kenmerken	Intrinsieke en persoonlijkheids-kenmerken/ mentaal/ criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie-technieken/ motieven	Modus operandi/ misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer/ dader)
						Samenwerking handlangers			

↩ Terug naar de overzichtspagina van deze bijlage



Afbeelding: Unsplash. (2017, 8 maart). https://unsplash.com/photos/person-writing-on-white-notebook-LtNvQHdKkmw

BIJLAGE 3

Inzichten uit de praktijkgerichte literatuur: dader- en slachtofferschap online criminaliteit

OPBOUW BIJLAGE

BIJLAGE 3: INZICHTEN UIT DE PRAKTIJKGERICHTE LITERATUUR

Bijlage 3.1: Daderschap

Bijlage 3.1.1: Algemene weerbaarheid
Bijlage 3.1.2: Hacking + mal-/ransomware
Bijlage 3.1.3: Online fraude
Bijlage 3.1.4: Online geweld/cyberpesten
Bijlage 3.1.5: Phishing
Bijlage 3.1.6: Sexting/sextortion/grooming
Bijlage 3.1.7: Overig

Bijlage 3.2: Slachtofferschap

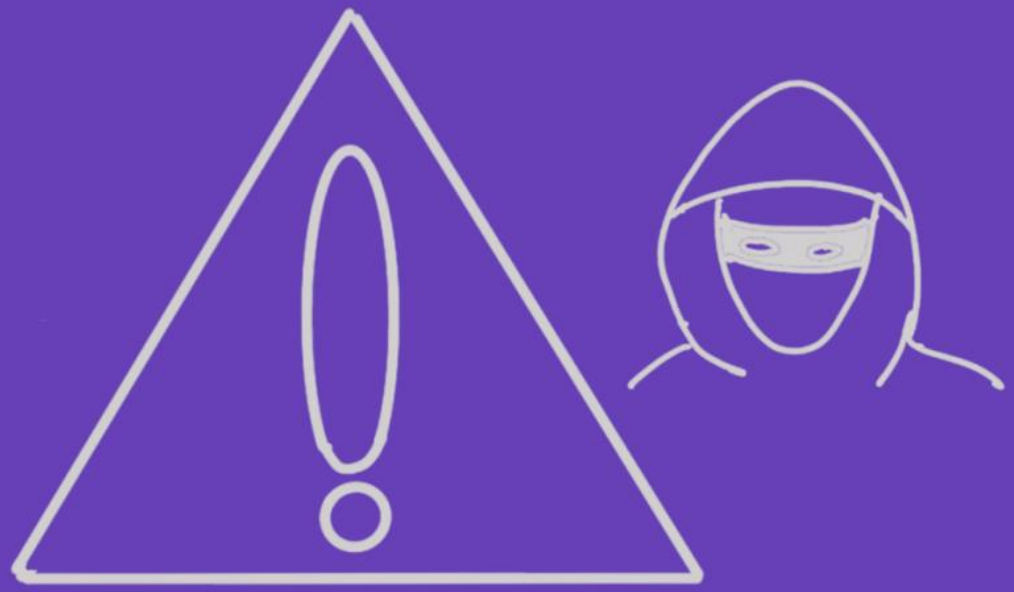
Bijlage 3.2.1: Algemene weerbaarheid
Bijlage 3.2.2: Hacking + mal-/ransomware
Bijlage 3.2.3: Online fraude
Bijlage 3.2.4: Online geweld/cyberpesten
Bijlage 3.2.5: Phishing
Bijlage 3.2.6: Sexting/sextortion/grooming
Bijlage 3.2.7: Overig

De resultaten zijn eveneens te raadplegen in Excel- en Word-format.
Daarnaast is het aparte eindrapport hier te vinden.
Onderstreepte woorden zijn linkjes naar de betreffende documenten.

Werken de linkjes niet? Mail dan a.u.b. naar e.land@saxion.nl of r.spithoven@saxion.nl.

ⓘ Klik op de paragraaftitels om naar de betreffende dia's te gaan

↩ Terug naar de inhoudsopgave



BIJLAGE 3.1

Inzichten uit de praktijkgerichte literatuur: daderschap online criminaliteit

Overzichten per delictstype

BIJLAGE 3.1.1: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

DADERS | Algemene weerbaarheid

DADERSCHAP | Algemene weerbaarheid

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | ALGEMENE WEERBAARHEID Totaal aantal interventies = 6			
Kwaliteit	**Aard van de interventie**	**Doelgroep**	**Voorbeelden (+ linkjes)**
Geëvalueerd, positief resultaat *Totaal = 1*	▪ Serious game = 1x	▪ Jongeren = 1x	▪ Framed, de cybergame
Geëvalueerd, negatief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, gemixte resultaten *Totaal = 2*	▪ Informatie/educatie = 1x ▪ Ondersteuning/hulp = 1x ▪ Serious game = 1x	▪ Jongeren = 2x	▪ Youth Cyber Team ▪ Cyber Explorers
Niet geëvalueerd, werking onbekend *Totaal = 3*	▪ Informatie/educatie = 3x ▪ Serious game = 2x	▪ Jongeren = 3x	▪ #BeCyberSmart ▪ NetSmartz ▪ Basicly
Niet geëvalueerd, wel veelbelovend/positieve signalen *Totaal = 0*	-	-	-

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.1.2: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

DADERSCHAP | Hacking + mal-/ransomware

DADERS | Hacking + mal-/ransomware

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | HACKING + MAL-/RANSOMWARE
Totaal aantal interventies = 10

Kwaliteit	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Geëvalueerd, positief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, negatief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, gemixte resultaten *Totaal = 1*	▪ Verstoring = 1x	▪ Jongeren = 1x	▪ Hack_Right
Niet geëvalueerd, werking onbekend *Totaal = 3*	▪ Informatie/educatie = 3x ▪ Bewustwordingscampagne = 1x ▪ Serious game = 1x	▪ Jongeren = 3x	▪ Leskaart Weerbaar Online ▪ Codekinderen.nl ▪ Hacker : HUNTER
Niet geëvalueerd, wel veelbelovend/positieve signalen *Totaal = 6*	▪ Informatie/educatie = 3x ▪ Evenement/bijeenkomst = 2x ▪ Verstoring = 2x ▪ Serious game = 1x ▪ Ondersteuning/hulp = 1x ▪ Bewustwordingscampagne = 1x	▪ Algemeen = 3x ▪ Jongeren = 3x	▪ Ethical Hacking ▪ Cyber24 ▪ re_B00TCMP ▪ Cyber Choices ▪ Operation Cookie Monster ▪ Operation Endgame

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.1.3: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

DADERS | Online fraude

DADERSCHAP | Online fraude | 1/2

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | ONLINE FRAUDE
Totaal aantal interventies = 14

Kwaliteit	Delictstype	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Geëvalueerd, positief resultaat *Totaal = 4*	Algemeen (3x), waarvan: ▪ Aan- en verkoopfraude = 2x ▪ Geldezels = 2x ▪ (Bank)helpdeskfraude = 1x ▪ Hulpvraag- en vriend-in-noodfraude = 1x	▪ Verstoring = 4x ▪ Bewustwordingscampagne = 1x ▪ Informatie/educatie = 1x ▪ Ondersteuning/hulp = 1x	▪ Algemeen = 3x ▪ Jongeren = 1x	▪ Lokale interventie voor geldezels ▪ Verstoring Tech Support Scam ▪ Buitengerechtelijke afdoening* ▪ Directe aansprakelijkheid
Geëvalueerd, negatief resultaat *Totaal = 0*		-	-	-
Geëvalueerd, gemixte resultaten *Totaal = 3*	Algemeen (3x), waarvan: ▪ Aan- en verkoopfraude = 2x ▪ Geldezels = 1x	▪ Verstoring = 2x ▪ Ondersteuning/hulp = 1x	▪ Algemeen = 2x ▪ Jongeren = 1x	▪ Youth Cyber Team ▪ Stopgesprek ▪ Lokaal daderschap

*Voor een aantal van deze interventies was het plaatsen van een linkje niet mogelijk i.v.m. verwijzing naar een (intern) document.

1/2

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.1.3: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

DADERSCHAP | Online fraude | 2/2

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | ONLINE FRAUDE

Totaal aantal interventies = 14

Kwaliteit	Delictstype	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Niet geëvalueerd, werking onbekend *Totaal = 2*	Algemeen (2x), waarvan: ▪ (Bank)helpdeskfraude = 1x ▪ Geldezels = 1x	▪ Bewustwordingscampagne = 1x ▪ Informatie/educatie = 1x	▪ Jongeren = 2x	▪ Leskaart Weerbaar Online ▪ #Selfmade? Cellmate!
Niet geëvalueerd, wel veelbelovend/ positieve signalen *Totaal = 5*	Algemeen (5x), waarvan: ▪ Geldezels = 3x ▪ (Bank)helpdeskfraude = 2x ▪ ID-Fraude = 2x ▪ Aan- en verkoopfraude = 1x ▪ Hulpvraag- en vriend-in-noodfraude = 1x ▪ Oplichting algemeen = 1x	▪ Verstoring = 3x ▪ Informatie/educatie = 2x ▪ Bewustwordingscampagne = 1x ▪ Ondersteuning/hulp = 1x ▪ Serious game = 1x	▪ Algemeen = 3x ▪ Jongeren = 2x	▪ Cyber24 ▪ Shitzooi ▪ Integrale Aanpak Online Fraude ▪ Blokkeren van spoofing door Finse autoriteiten ▪ #Don'tBeAMule en EMMA

2/2

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.1.4: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

DADERSCHAP | Online geweld/cyberpesten

DADERS | Online geweld/ cyberpesten

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | ONLINE GEWELD/CYBERPESTEN
Totaal aantal interventies = 7

Kwaliteit	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Geëvalueerd, positief resultaat *Totaal = 1*	▪ Informatie/educatie = 1x	▪ Jongeren = 1x	▪ Risk Factory
Geëvalueerd, negatief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, gemixte resultaten *Totaal = 1*	▪ Ondersteuning/hulp = 1x	▪ Jongeren = 1x	▪ Youth Cyber Team
Niet geëvalueerd, werking onbekend *Totaal = 3*	▪ Informatie/educatie = 3x ▪ Serious game = 1x	▪ Jongeren = 3x	▪ Leskaart Weerbaar Online ▪ NetSmartz ▪ Basicly
Niet geëvalueerd, wel veelbelovend/positieve signalen *Totaal = 2*	▪ Informatie/educatie = 2x ▪ Verstoring = 1x	▪ Jongeren = 2x	▪ Respect Online van Halt. ▪ It's Up To You

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.1.5: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

DADERS | Phishing

DADERSCHAP | Phishing

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | PHISHING Totaal aantal interventies = 3			
Kwaliteit	**Aard van de interventie**	**Doelgroep**	**Voorbeelden (+ linkjes)**
Geëvalueerd, positief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, negatief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, gemixte resultaten *Totaal = 0*	-	-	-
Niet geëvalueerd, werking onbekend *Totaal = 1*	▪ Bewustwordingscampagne = 1x	▪ Jongeren = 1x	▪ #Selfmade? Cellmate!
Niet geëvalueerd, wel veelbelovend/positieve signalen *Totaal = 2*	▪ Verstoring = 2x ▪ Informatie/educatie = 1x ▪ Ondersteuning/hulp = 1x	▪ Algemeen = 2x	▪ Project BigPhish ▪ Integrale Aanpak Online Fraude

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.1.6: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

DADERSCHAP | Sexting/sextortion/grooming

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | SEXTING/SEXTORTION/GROOMING
Totaal aantal interventies = 6

Kwaliteit	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Geëvalueerd, positief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, negatief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, gemixte resultaten *Totaal = 0*	-	-	-
Niet geëvalueerd, werking onbekend *Totaal = 1*	▪ Informatie/educatie = 1x ▪ Serious game = 1x	▪ Jongeren = 1x	▪ NetSmartz
Niet geëvalueerd, wel veelbelovend/ positieve signalen *Totaal = 5*	▪ Informatie/educatie = 4x ▪ Ondersteuning/hulp = 1x ▪ Serious game = 1x ▪ Tool = 1x ▪ Verstoring = 1x	▪ Jongeren = 5x	▪ Cyber24 ▪ Shitzooi ▪ Respect Online van Halt. ▪ Toolkit L.O.V.E. Online van Halt. ▪ Sextoooh

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.1.7: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

DADERS | Overig

DADERSCHAP | Overig

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | DADERSCHAP | OVERIG
Totaal aantal interventies = 3

Kwaliteit	Delictstype	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Geëvalueerd, positief resultaat *Totaal = 0*	-	-	-	-
Geëvalueerd, negatief resultaat *Totaal = 0*	-	-	-	-
Geëvalueerd, gemixte resultaten *Totaal = 1*	▪ Desinformatie = 1x ▪ Exposen = 1x	▪ Ondersteuning/hulp = 1x	▪ Jongeren = 1x	▪ Youth Cyber Team
Niet geëvalueerd, werking onbekend *Totaal = 0*	-	-	-	-
Niet geëvalueerd, wel veelbelovend/ positieve signalen *Totaal = 2*	▪ DDoS = 2x	▪ Bewustwordingscampagne = 2x ▪ Verstoring = 1x	▪ Algemeen = 2x	▪ Google Ads campagne ▪ Operation PowerOFF

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.2

Inzichten uit de praktijkgerichte literatuur: slachtofferschap online criminaliteit

Overzichten per delictstype

BIJLAGE 3.2.1: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERSCHAP | Algemene weerbaarheid | 1/2

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | ALGEMENE WEERBAARHEID

Totaal aantal interventies = 41

Kwaliteit	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Geëvalueerd, positief resultaat *Totaal = 8*	▪ Ondersteuning/hulp = 5x ▪ Scan = 5x ▪ Informatie/educatie = 4x ▪ Bewustwordings-campagne = 2x ▪ Serious game = 1x	▪ Bedrijven/ ondernemers = 4x ▪ Jongeren = 2x ▪ Gemeenten = 1x ▪ Overig (1x): Agrarische sector	▪ Project Troje ▪ Cybersecurityster ▪ Cyberchef ▪ Friese agrarische sector cyberproof ▪ Cyberbuddies ▪ Digitale Inclusie ▪ Evidence based cybersecurity gedragsinterventie (...) ▪ Risk Factory
Geëvalueerd, negatief resultaat *Totaal = 1*	▪ Ondersteuning/hulp = 1x	▪ Bedrijven/ ondernemers = 1x	▪ Ambassadeursnetwerk mkb
Geëvalueerd, gemixte resultaten *Totaal = 11*	▪ Ondersteuning/hulp = 8x ▪ Informatie/educatie = 7x ▪ Evenement/bijeenkomst = 2x ▪ Serious game = 2x ▪ Scan = 1x	▪ Bedrijven/ ondernemers = 5x ▪ Algemeen = 3x ▪ Jongeren = 3x ▪ Gemeenten = 2x ▪ Senioren = 1x	▪ Cyber Sessions ▪ Sterkere Schakels Versterken de Keten! ▪ Digitale Buurtambassadeurs ▪ Pilot Multichannel aanpak (...) ▪ Youth Cyber Team ▪ Living Lab ▪ Brede aanpak digitale weerbaarheid (...) ▪ Regionaal Expertteam Digitale Veiligheid ▪ Serious game cyberweerbaarheid laaggeletterden ▪ Digitaal Veilig in Limburg ▪ Cyber Explorers

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.2.1: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERSCHAP | Algemene weerbaarheid | 2/2

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | ALGEMENE WEERBAARHEID

Totaal aantal interventies = 41

Kwaliteit	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Niet geëvalueerd, werking onbekend *Totaal = 10*	▪ Informatie/educatie = 9x ▪ Serious game = 6x ▪ Ondersteuning/hulp = 4x ▪ Bewustwordingscampagne = 1x ▪ Evenement/bijeenkomst = 1x	▪ Jongeren = 6x ▪ Algemeen = 3x ▪ Bedrijven/ ondernemers = 3x ▪ Senioren = 1x ▪ Overig (1x): Laag-geletterden	▪ Digitaal Veilig in de Wijk ▪ Dordrecht Digitaal Weerbaar ▪ Storytelling Cybercrime ▪ #BeCyberSmart ▪ CyberSprinters ▪ STOP.THINK.CONNECT. ▪ NetSmartz ▪ De InternetHelden ▪ De Kiesraad ▪ Cyber Crime the Game
Niet geëvalueerd, wel veelbelovend/ positieve signalen *Totaal = 11*	▪ Informatie/educatie = 8x ▪ Ondersteuning/hulp = 5x ▪ Serious game = 3x ▪ Evenement/bijeenkomst = 2x ▪ Bewustwordingscampagne = 2x ▪ Tool = 2x	▪ Jongeren = 5x ▪ Algemeen = 4x ▪ Bedrijven/ ondernemers = 2x ▪ Gemeenten = 1x ▪ Overig (1x): Digitaal minder-vaardigen	▪ Cybersnackbox ▪ Gastveilig Hazeldonk ▪ Veilig digitaal op weg naar de brugklas ▪ Echt niet vandaag ▪ Unlock Digitale Weerbaarheid ▪ HackShield ▪ European Cyber Security Month ▪ Online Veilig ▪ #DNTF, Digitaal Niet Te Foppen ▪ MediaMasters ▪ Safeonweb.be

2/2

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.2.2: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERSCHAP | Hacking + mal-/ransomware | 1/2

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | HACKING + MAL-/RANSOMWARE

Totaal aantal interventies = 27

Kwaliteit	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Geëvalueerd, positief resultaat *Totaal = 3*	▪ Informatie/educatie = 3x ▪ Ondersteuning/hulp = 2x ▪ Serious game = 1x ▪ Tool = 1x ▪ Verstoring = 1x	▪ Algemeen = 1x ▪ Bedrijven/ ondernemers = 1x ▪ Jongeren = 1x	▪ Hackhelpdesk ▪ Digitale Inclusie ▪ NoMoreRansom
Geëvalueerd, negatief resultaat *Totaal = 1*	▪ Bewustwordingscampagne = 1x ▪ Informatie/educatie = 1x	▪ Algemeen = 1x	▪ Doe je Updates
Geëvalueerd, gemixte resultaten *Totaal = 2*	▪ Bewustwordingscampagne = 1x ▪ Informatie/educatie = 2x ▪ Evenement/bijeenkomst = 1x ▪ Ondersteuning/hulp = 1x	▪ Algemeen = 1x ▪ Bedrijven/ ondernemers = 1x	▪ Dubbel Beveiligd is Dubbel zo Veilig ▪ Living Lab

BIJLAGE 3.2.2: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERSCHAP | Hacking + mal-/ransomware | 2/2

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | HACKING + MAL-/RANSOMWARE

Totaal aantal interventies = 27

Kwaliteit	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Niet geëvalueerd, werking onbekend *Totaal = 13*	▪ Informatie/educatie = 8x ▪ Bewustwordingscampagne = 5x ▪ Tool = 4x ▪ Ondersteuning/hulp = 3x ▪ Serious game = 3x	▪ Algemeen = 7x ▪ Jongeren = 3x ▪ Bedrijven/ ondernemers = 2x ▪ Gemeenten = 1x ▪ Senioren = 1x ▪ Overig (1x): Drinkwatersector	▪ Alisson ▪ Cyberoefenpakket VNG ▪ Tool Cyberweerbaarheid ▪ Geflasht! ▪ Laat je niet Hack maken ▪ Laat je niet Interneppen ▪ Check je Hack ▪ No More Leaks ▪ CyberSprinters ▪ STOP.THINK.CONNECT. ▪ Have I Been Pwned? ▪ #EchtNep? ▪ #FerryVeilig
Niet geëvalueerd, wel veelbelovend/positieve signalen *Totaal = 8*	▪ Informatie/educatie = 6x ▪ Ondersteuning/hulp = 3x ▪ Serious game = 2x ▪ Bewustwordingscampagne = 1x ▪ Tools = 1x	▪ Jongeren = 4x ▪ Algemeen = 4x	▪ Mijn Cyberrijbewijs ▪ Hackers de Baas ▪ Unlock Digitale Weerbaarheid ▪ Cyber24 ▪ HackShield ▪ Stop Ransomware ▪ Online Veilig ▪ Safeonweb.be

2/2

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.2.3: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERSCHAP | Online fraude | 1/3

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | ONLINE FRAUDE

Totaal aantal interventies = 34

Kwaliteit	Delictstype	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Geëvalueerd, positief resultaat *Totaal = 6*	Algemeen (6x), waarvan: ▪ (Bank)helpdeskfraude = 3x ▪ Datingfraude = 2x ▪ Aan- en verkoopfraude = 1x ▪ Geldezels = 1x ▪ Hulpvraag- en vriend-in-noodfraude = 1x	▪ Informatie/educatie = 2x ▪ Ondersteuning/hulp = 2x ▪ Tool = 2x ▪ Bewustwordings-campagne = 1x ▪ Verstoring = 1x	▪ Algemeen = 4x ▪ Senioren = 2x ▪ Jongeren = 1x ▪ Overig (elk 1x) = Alleenstaanden, Kwetsbaren	▪ Verstoring Tech Support Scam ▪ Bank voor de Klas en F-Game ▪ Echt of nep? Interactieve film ▪ Check je (Ver)koper ▪ ING x Geldfit ▪ Check het gesprek
Geëvalueerd, negatief resultaat *Totaal = 1*	-	-	-	-
Geëvalueerd, gemixte resultaten *Totaal = 4*	Algemeen (4x), waarvan: ▪ (Bank)helpdeskfraude = 1x ▪ Hulpvraag- en vriend-in-noodfraude = 1x ▪ Geldezels = 1x	▪ Ondersteuning/hulp = 3x ▪ Informatie/educatie = 1x ▪ Serious game = 1x	▪ Algemeen = 2x ▪ Bedrijven/ ondernemers = 2x ▪ Jongeren = 2x ▪ Senioren = 1x	▪ Podcast Digitaal Beroofd ▪ Youth Cyber Team ▪ Serious game cyberweerbaarheid laaggeletterden ▪ Digitaal veilig in Limburg

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.2.3: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERS | Online fraude

SLACHTOFFERSCHAP | Online fraude | 2/3

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | ONLINE FRAUDE
Totaal aantal interventies = 34

Kwaliteit	Delictstype	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Niet geëvalueerd, werking onbekend *Totaal = 10*	Algemeen (10x), waarvan: ▪ Oplichting algemeen = 5x ▪ Hulpvraag- en vriend-in-noodfraude = 4x ▪ Aan- en verkoopfraude = 3x ▪ (Bank)helpdeskfraude = 2x ▪ Datingfraude = 2x ▪ ID-fraude = 2x ▪ Beleggingsfraude = 1x ▪ Geldezels = 1x	▪ Informatie/educatie = 8x ▪ Bewustwordings-campagne = 7x ▪ Tool = 3x ▪ Ondersteuning/hulp = 3x ▪ Verstoring = 1x	▪ Algemeen = 8x ▪ Jongeren = 2x ▪ Bedrijven/ ondernemers = 1x ▪ Senioren = 1x	▪ Check je Aanbieder ▪ Verlies je hart niet aan datingfraude ▪ Voorkom fraude ▪ ScamCheck ▪ Tool Cyberweerbaarheid ▪ Geflasht! ▪ Laat je niet Interneppen ▪ Maatregel Knab ▪ #EchtNep? ▪ #FerryVeilig

2/3

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.2.3: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERSCHAP | Online fraude | 3/3

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | ONLINE FRAUDE
Totaal aantal interventies = 34

Kwaliteit	Delictstype	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Niet geëvalueerd, wel veel-belovend/ positieve signalen *Totaal = 14*	Algemeen (14x), waarvan: ▪ Oplichting algemeen = 5x ▪ (Bank)helpdeskfraude = 3x ▪ Geldezels = 3x ▪ Hulpvraag- en vriend-in-noodfraude = 3x ▪ ID-fraude = 3x ▪ Aan- en verkoopfraude = 1x ▪ Datingfraude = 1x	▪ Informatie/educatie = 10x ▪ Tool = 5x ▪ Bewustwordings-campagne = 4x ▪ Ondersteuning/hulp = 4x ▪ Serious game = 3x ▪ Meldpunt = 2x ▪ Verstoring = 1x	▪ Algemeen = 10x ▪ Jongeren = 3x ▪ Bedrijven/ ondernemers = 2x ▪ Senioren = 1x	▪ Webinar Weerbaar tegen Phishing ▪ Verliefd op de persoon? Of op het profiel? ▪ Mijn Cyberrijbewijs ▪ Shitzooi ▪ LMIO + pakjedealsnu.nl ▪ Unlock Digitale Weerbaarheid ▪ Cyber24 ▪ Integrale Aanpak Online Fraude ▪ CIFAS ▪ Scam Signal ▪ Scam Spotter ▪ ScamShield ▪ Online Veilig ▪ Safeonweb.be

BIJLAGE 3.2.4: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERSCHAP | Online geweld/cyberpesten

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | ONLINE GEWELD/CYBERPESTEN
Totaal aantal interventies = 3

Kwaliteit	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Geëvalueerd, positief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, negatief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, gemixte resultaten *Totaal = 1*	▪ Ondersteuning/hulp = 1x	▪ Jongeren = 1x	▪ Youth Cyber Team
Niet geëvalueerd, werking onbekend *Totaal = 1*	▪ Informatie/educatie = 1x ▪ Serious game = 1x	▪ Jongeren = 1x	▪ NetSmartz
Niet geëvalueerd, wel veelbelovend/positieve signalen *Totaal = 1*	▪ Serious game = 1x	▪ Jongeren = 1x	▪ MediaMasters

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.2.5: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERSCHAP | Phishing | 1/2

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | PHISHING Totaal aantal interventies = 19			
Kwaliteit	**Aard van de interventie**	**Doelgroep**	**Voorbeelden (+ linkjes)**
Geëvalueerd, positief resultaat *Totaal = 2*	▪ Informatie/educatie = 2x ▪ Serious game = 1x	▪ Jongeren = 1x ▪ Senioren = 1x	▪ Digitale Inclusie ▪ Echt of Nep? Interactieve training
Geëvalueerd, negatief resultaat *Totaal = 0*	x	x	x
Geëvalueerd, gemixte resultaten *Totaal = 2*	▪ Ondersteuning/hulp = 2x ▪ Serious game = 1x	▪ Algemeen = 1x ▪ Bedrijven/ ondernemers = 1x ▪ Jongeren = 1x ▪ Senioren = 1x	▪ Serious game cyberweerbaarheid laaggeletterden ▪ Digitaal Veilig in Limburg

BIJLAGE 3.2.5: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERSCHAP | Phishing | 2/2

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | PHISHING
Totaal aantal interventies = 19

Kwaliteit	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Niet geëvalueerd, werking onbekend *Totaal = 6*	▪ Informatie/educatie = 5x ▪ Bewustwordingscampagne = 3x ▪ Ondersteuning/hulp = 3x ▪ Serious game = 3x ▪ Tool = 2x	▪ Algemeen = 4x ▪ Jongeren = 3x ▪ Bedrijven/ondernemers = 2x ▪ Senioren = 1x	▪ ScamCheck ▪ Laat je niet Interneppen ▪ #BeCyberSmart ▪ CyberSprinters ▪ #EchtNep? ▪ Cyber Crime the Game ▪ Safeonweb.be
Niet geëvalueerd, wel veelbelovend/positieve signalen *Totaal = 9*	▪ Informatie/educatie = 7x ▪ Ondersteuning/hulp = 4x ▪ Bewustwordingscampagne = 2x ▪ Serious game = 2x ▪ Tool = 1x ▪ Verstoring = 1x	▪ Algemeen = 4x ▪ Jongeren = 2x ▪ Senioren = 1x	▪ Webinar Weerbaar tegen Phishing ▪ Hackers de Baas ▪ Eerst Checken, dan Klikken ▪ Unlock Digitale Weerbaarheid ▪ Integrale Aanpak Online Fraude ▪ HackShield ▪ ScamShield ▪ Online Veilig

BIJLAGE 3.2.6: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERSCHAP | Sexting/sextortion/grooming

SLACHTOFFERS | Sexting/ sextortion/ grooming

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | SEXTING/SEXTORTION/GROOMING Totaal aantal interventies = 9			
Kwaliteit	**Aard van de interventie**	**Doelgroep**	**Voorbeelden (+ linkjes)**
Geëvalueerd, positief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, negatief resultaat *Totaal = 0*	-	-	-
Geëvalueerd, gemixte resultaten *Totaal = 0*	-	-	-
Niet geëvalueerd, werking onbekend *Totaal = 2*	▪ Informatie/educatie = 2x ▪ Serious game = 2x ▪ Ondersteuning/hulp = 1x	▪ Jongeren = 2x	▪ NetSmartz ▪ De Kiesraad
Niet geëvalueerd, wel veelbelovend/ positieve signalen *Totaal = 7*	▪ Informatie/educatie = 6x ▪ Serious game = 3x ▪ Ondersteuning/hulp = 2x	▪ Jongeren = 6x ▪ Algemeen = 1x	▪ Mijn Cyberrijbewijs ▪ Escaperoombus/Bl@ckmail ▪ Shitzooi ▪ Toolkit L.O.V.E. Online van Halt. ▪ Unlock Digitale Weerbaarheid ▪ Cyber24 ▪ WTFFF?! X Stukje van Mij

↩ Terug naar de overzichtspagina van deze bijlage

BIJLAGE 3.2.7: INZICHTEN PRAKTIJKGERICHTE LITERATUUR

SLACHTOFFERS | Overig

SLACHTOFFERSCHAP | Overig

INZICHTEN PRAKTIJKGERICHTE LITERATUUR | SLACHTOFFERSCHAP | OVERIG
Totaal aantal interventies = 5

Kwaliteit	Delictstype	Aard van de interventie	Doelgroep	Voorbeelden (+ linkjes)
Geëvalueerd, positief resultaat *Totaal = 0*	-	-	-	-
Geëvalueerd, negatief resultaat *Totaal = 1*	▪ Desinformatie = 1x	▪ Serious game = 1x	▪ Jongeren = 1x	▪ Juice of (fake-)news?
Geëvalueerd, gemixte resultaten *Totaal = 2*	▪ DDoS = 1x ▪ Desinformatie = 1x ▪ Exposen = 1x	▪ Informatie/educatie = 1x ▪ Ondersteuning/hulp = 1x	▪ Algemeen = 1x ▪ Jongeren = 1x	▪ Podcast Digitaal Beroofd ▪ Youth Cyber Team
Niet geëvalueerd, werking onbekend *Totaal = 0*	-	-	-	-
Niet geëvalueerd, wel veelbelovend/ positieve signalen *Totaal = 2*	▪ Desinformatie = 1x ▪ Doxing = 1x ▪ Hate speech = 1x	▪ Informatie/educatie = 2x	▪ Algemeen = 1x ▪ Jongeren = 1x	▪ Mijn Cyberrijbewijs ▪ Unlock Digitale Weerbaarheid

↩ Terug naar de overzichtspagina van deze bijlage