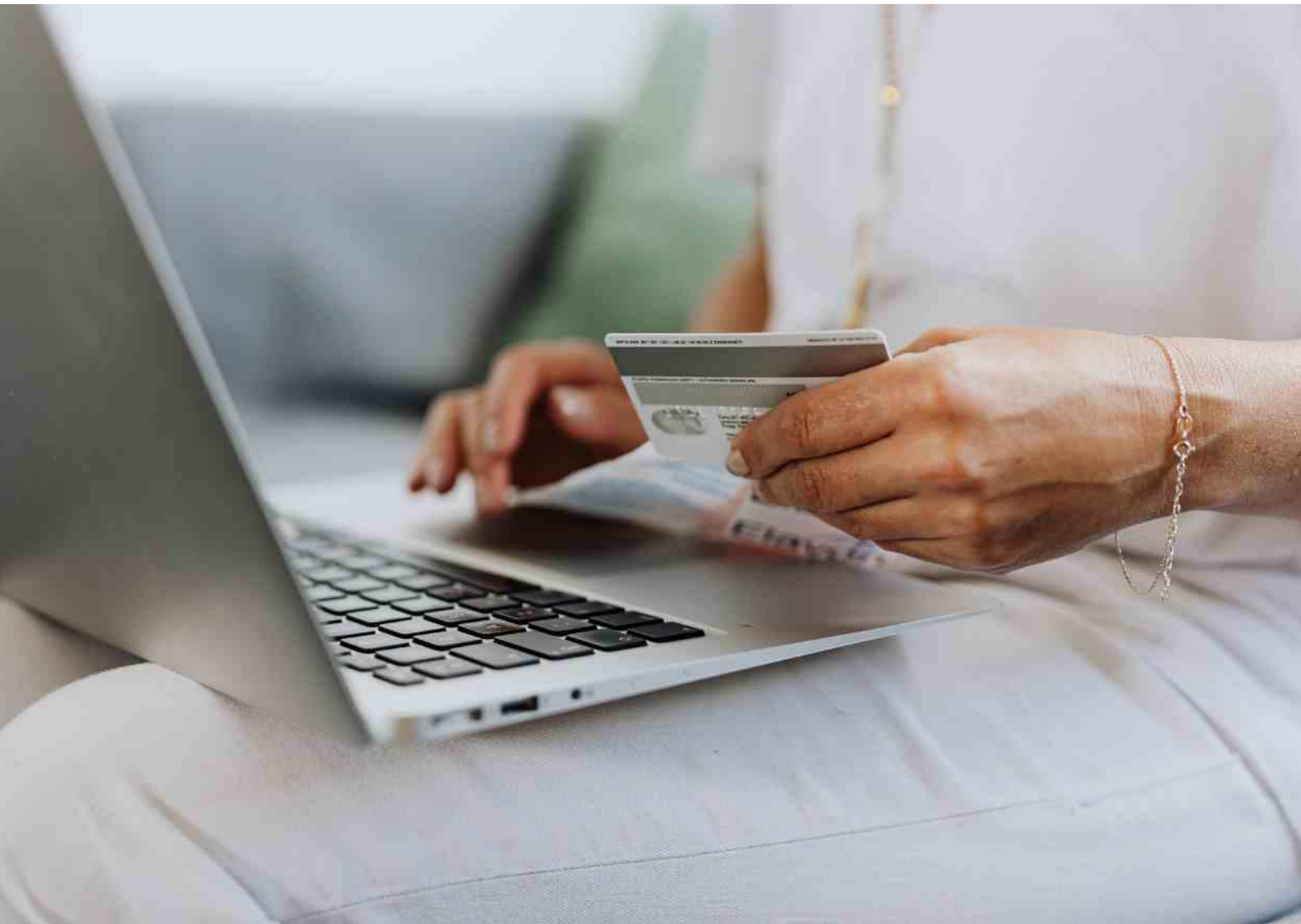
Ministerie van Justitie en Veiligheid

Actieplan Integrale Aanpak Online Fraude



Beleid online fraude

Online fraude is een groeiend maatschappelijk probleem. Naast financiële schade voor slachtoffers - zowel bij burgers als in het bedrijfsleven - kan online fraude ook emotionele of psychische schade veroorzaken bij slachtoffers en hun omgeving. Het schaadt ook het vertrouwen in digitalisering terwijl dit juist veel voordelen heeft. Het is van groot belang om met brede preventie, doeltreffende interventies en opvolging door politie en openbaar ministerie een kentering aan te brengen in deze ontwikkeling.

Integrale aanpak online fraude

Deze kentering kan alleen aangebracht worden als alle partners, die bij de aanpak van online fraude betrokken zijn, meerjarig en structureel samenwerken. Het doel van de integrale aanpak is partners in hun eigen aanpak sneller, gerichter, daadkrachtiger, effectiever en langduriger succesvol te laten zijn. De integrale aanpak is een samenwerking waarin betrokken partners daartoe acties met elkaar afspreken (binnen hun bevoegdheden). Daarmee draagt de integrale aanpak bij aan de gedeelde ambitie om het aantal slachtoffers van online fraude te verminderen. Dit complexe vraagstuk vraagt van eenieder een lange adem en duurzame inzet van menskracht en middelen.

Gezamenlijke doelstelling

De integrale aanpak online fraude heeft als doel om meerjarig gezamenlijk de krachten te bundelen, de onderlinge informatiepositie te verstevigen, het kennisniveau te verhogen, te weten en te doen wat werkt om sneller, flexibeler en effectiever op te kunnen treden tegen online fraude teneinde het aantal slachtoffers te verminderen.

Prioritaire vormen online fraude

Online fraude kent vele vormen, die voortdurend in beweging zijn. Om gericht te werk te gaan in het actieplan wordt bij de start van het actieplan de focus gelegd op de door de partners benoemde vijf grote fraudevormen:

- aan- en verkoopfraude
- phishing met betaalgegevens
- hulpvraagfraude
- (bank)helpdeskfraude
- identiteitsfraude

Fraudevormen van het actieplan nader toegelicht:

Aan- en verkoopfraude: Betreft fraude via bijvoorbeeld online-handelsplaatsen of valse webwinkels. Bij aankoopfraude maakt de verkopende partij er de gewoonte van om producten of diensten niet te leveren na betaling door het slachtoffer. Bij verkoopfraude worden goederen of diensten wel geleverd door het slachtoffer, maar maakt de ontvanger er de gewoonte van om daar niet voor te betalen.

Phishing met betaalgegevens: De fraudeur probeert om via e-mail en sms vertrouwelijke informatie, zoals bankgegevens, wachtwoorden, en creditcardnummers te bemachtigen.

Vriend-in-noodfraude (ook wel: hulpvraagfraude): De fraudeur doet zich voor als een bekende die in geldnood is en vraagt om geld over te maken. Dit gebeurt meestal via instant messaging apps, e-mail, SMS en sociale media.

(Bank)helpdeskfraude: Bij deze vorm van fraude doet een fraudeur zich voor als een medewerker van de overheid of van een bedrijf. Meestal wordt het slachtoffer door de fraudeur benaderd, maar soms komt het slachtoffer in zijn zoektocht per ongeluk uit bij een frauduleuze helpdesk. De fraudeur heeft interactie met het slachtoffer en zet het slachtoffer aan tot het doen van een overboeking, afgeven van betaalmiddelen of het installeren van ‘Remote Access Tooling’, waarna er frauduleuze transacties plaatsvinden.

Identiteitsfraude: De fraudeur neemt andermans identiteit of een gecreëerde, fictieve identiteit aan om daarmee geld en/of goederen te verwerven.


ACCESS
DENIED

Thema's actieplan

Het actieplan geeft aan met welke opdracht de integrale aanpak wordt gestart op een aantal thema's:

- zicht op fraude: het verkrijgen en delen van inzichten in aard en omvang, modus operandi, relevante ontwikkelingen, trends en cijfers over dader- en slachtofferschap, internationale ontwikkelingen en uiteraard de effecten van beleid en interventies met als doel om beter en sneller in te kunnen spelen op ontwikkelingen bij online fraude;
- gegevensdeling: het vinden van mogelijkheden om (cross-sectoraal) gegevens uit te wisselen om daders te verhinderen om slachtoffers te maken en/of daders op te sporen;
- (technische) barrières & interventies: het opwerpen van barrières en het ontwikkelen van vroege signalering en interventies om fraude te voorkomen, potentiële slachtoffers te waarschuwen en potentiële daders te weren;
- opvolging politie en openbaar ministerie: het versterken van de aanpak door politie en openbaar ministerie op grond van onder andere de Veiligheidsagenda 2023-2026;
- weerbaarheid/preventie: het versterken en benutten van de mogelijkheden van burgers en bedrijven om geen slachtoffer van online fraude te worden;
- hulp aan slachtoffers: het ondersteunen van burgers en bedrijven die slachtoffer van online fraude zijn geworden.

Het actieplan geeft richting aan de samenwerking en zorgt voor prioriteitstelling. Hierbij is gebruik gemaakt van de uitkomsten van het onderzoek van de Universiteit van Twente naar fraudevictimisatie in Nederland en de opbrengsten van werksessies die het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) heeft begeleid. Het actieplan vormt nadrukkelijk geen 'harnas' en kan worden aangepast als actuele ontwikkelingen hierom vragen. Het actieplan zelf bestrijkt de duur van de integrale aanpak. De totstandkoming van de beoogde resultaten binnen het actieplan kent uiteraard een planning, die vooralsnog ziet op 2023. In het najaar van 2023 worden de integrale aanpak en het actieplan geëvalueerd om te bezien welke wijzigingen nodig zijn om succes van de integrale aanpak te vergroten.

Governance

In de integrale aanpak wordt op drie niveaus samengewerkt:

- bestuurlijk: waar nodig en wenselijk zal door de minister van Justitie en Veiligheid en haar ambtgenoten met bestuurders van aan de integrale aanpak deelnemende partners ad hoc worden overlegd om de integrale aanpak op koers te houden. Verder wordt op bestuurlijk niveau jaarlijks een conferentie georganiseerd voor bestuurders (en beleidsmakers) van een veel grotere kring van organisaties, die betrokken zijn bij de aanpak van online fraude. Daarin wordt overleg gecombineerd met aandacht voor onder andere innovaties, nieuwe vormen van online fraude, effectieve maatregelen, uitkomsten van onderzoek.
- beleid: de integrale aanpak kent een kerngroep, waarin verschillende partners deelnemen, die zorgt voor de formulering en het maken van afspraken ten aanzien van het actieplan, die zorgt voor deelname aan de werkgroepen, bijeenkomsten en overleggen om resultaten te realiseren, die de voortgang van werkzaamheden monitort en die bestuurlijke overleggen voorbereidt. Daarnaast is er een veel grotere kring van organisaties, betrokken bij de aanpak van online fraude, die wordt geïnformeerd en bevraagd om bijvoorbeeld deel te nemen aan werkgroepen.
- werkgroepen/bijeenkomsten: de integrale aanpak kent een divers samenstel van werkgroepen, bijeenkomsten en overleggen waar experts van relevante organisaties met elkaar werken aan de totstandkoming van maatregelen in de aanpak van online fraude. In de werkgroepen komen die partners samen die bepalend zijn voor een effectieve aanpak. Partners nemen deel afhankelijk van hun betrokkenheid waarbij overlap met vergelijkbare overleggen wordt voorkomen.

Partners kerngroep

Politie, Openbaar Ministerie, VNO-NCW/MKB Nederland, Vodiom, Consumentenbond, Nederlandse Vereniging van Banken (NVB), COIN, Thuiswinkel.org, Meta, Vereniging Nederlandse Gemeenten (VNG) en de ministeries van Economische Zaken en Klimaat (EZK), van Financiën (FIN) en van Justitie en Veiligheid (JenV).

Partners in de integrale aanpak

Veel organisaties hebben aan de voorbereiding van de integrale aanpak bijgedragen, zoals het Centrum voor Criminaliteitspreventie (CCV), Landelijk Meldpunt Internet Oplichting (LMIO), Electronic Crimes Taskforce (ECTF) de Fraudehelpdesk, Autoriteit Consument en Markt (ACM), Slachtofferhulp Nederland, Marktplaats, ECP, SeniorenWeb, Algemeen Nederlandse Bond voor Ouderen (ANBO), SIDN, Veiligheidsalliantie Rotterdam en verschillende wetenschappers. De werkzaamheden in de integrale aanpak staan vanzelfsprekend open voor deelname door andere partners die een bijdrage willen leveren aan de aanpak van online fraude. Een e-mailbericht naar onlinefraude@minjenv.nl volstaat.

Rol JenV

Het ministerie van JenV is verantwoordelijk voor de beleidsontwikkeling ten aanzien van online fraude. Daarnaast voert het ministerie de regie op de integrale aanpak. De daartoe ingerichte projectgroep maakt voorstellen voor de actielijnen en stemt deze af in de kerngroep. De projectgroep zorgt tevens voor de meerjarige samenwerking in de integrale aanpak met bijvoorbeeld budget, communicatie en informatie. Tenslotte zorgt de projectgroep voor samenhang in de werkzaamheden van de integrale aanpak met gerelateerde beleidsterreinen en voor agendering op politiek niveau. Daarnaast draagt het ministerie aan de aanpak van online fraude bij door bijvoorbeeld op het gebied van gegevensdeling contact met de Autoriteit Persoonsgegevens te houden en vragen rondom de rechtsgrondslag voor gegevensdeling te beantwoorden. Het ministerie treedt ook op als opdrachtgever voor onderzoek naar online fraude of voor publiekscampagnes.

ACTIEPLAN

Het actieplan van de integrale aanpak online fraude heeft zowel een duurzaam als een dynamisch karakter. We kiezen hiermee voor een heldere koers die wel tussentijds kan worden aangescherpt en/of bijgesteld. Voor deze aanscherping is het zaak om voortdurend de voortgang te monitoren en periodiek te besluiten over bijstelling van het actieplan en daarmee de inzet van de partners voor de verschillende maatregelen. Daarmee behouden we ruimte om mee te bewegen met ontwikkelingen binnen het telkens veranderende fenomeen van online fraude.

Dit actieplan van de integrale aanpak online fraude moet worden gezien als een 'plus' bovenop de reeds lopende en ingezette activiteiten van alle partners. Het is geenszins de bedoeling om bestaande initiatieven onder de regie van de integrale aanpak te laten vallen en bestaande inzet van en samenwerking tussen partners wordt dan ook blijvend gestimuleerd. Met partners is afgesproken om resultaten, opbrengsten en knelpunten van aanpalende trajecten onderling actief te delen en elkaar te informeren zodat ook nauwlettend kan worden gemonitord welke activiteiten helpend en effectief zijn bij de bestrijding van online fraude. Daarbij wordt specifiek aandacht gegeven aan het leren van ontwikkelingen en kennis vanuit het buitenland. Daar waar voor een activiteit of resultaat de integrale aanpak van toegevoegde waarde is of noodzakelijk blijkt kan een actie worden opgenomen in het actieplan. In samenspraak met betrokken partners is een prioritering aangebracht van acties die vanuit de integrale aanpak als eerste moeten worden opgepakt. Dit actieplan is aan ontwikkeling en prioritering onderhevig en wordt jaarlijks herijkt.

Het is tenslotte belangrijk om aandacht te hebben voor de samenhang met overlappende trajecten, programma's en beleidsterreinen en daar waar mogelijk de krachten te bundelen.

1. Zicht op fraude

Doelstelling

Het fenomeen online fraude kent niet alleen veel gedaanten maar verandert ook voortdurend. Om online fraude gerichter en doeltreffender te kunnen voorkomen en bestrijden is het voor partijen uit de aanpak van online fraude nodig om beter zicht te hebben op de verschillende verschijningsvormen en trends. Niet alleen is het van belang deze ontwikkelingen te kennen en de oorzaken te onderzoeken, het is ook van belang te kijken naar patronen in de verschillende verschijningsvormen, de modus operandi en de slachtoffer- en dadertypen. Tegelijkertijd is het van belang om deze kennis en informatie over de aanpak van online fraude snel te kunnen vinden, te kunnen plaatsen en uit te kunnen wisselen en dat er afspraken worden gemaakt over wat er wordt gedaan met deze informatie en monitoring. Partijen, verbonden aan de integrale aanpak online fraude, zetten met elkaar in op het meer en beter delen van informatie op het gebied van (nieuwe) trends, modus operandi, cijfers en fraudevormen zodat partners in de aanpak van online fraude optimaal kunnen functioneren, slagkrachtig kunnen optreden en tijdig kunnen inspelen op veranderingen.

Resultaat	Actie	Planning	Kerngroep/werkgroep/bijeenkomst
Uitwisseling informatie over trends, MO's en cijfers	Inrichting werkgroep trends en cijfers	Q1 2023	Werkgroep informatie-uitwisseling
	Afspraken uitwisseling informatie over trends, MO's en cijfers	Q1 2023	Werkgroep informatie-uitwisseling
	Opdracht uitwerking voorstel 'dashboard'	Q1 2023	Werkgroep informatie-uitwisseling
	Factsheet trends en cijfers	Q2 en Q4 2023	Werkgroep informatie-uitwisseling
Verdieping kennis over online fraude	Inventarisatie bestaande en gewenste onderzoeken en monitors	Q1 2023	Werkgroep informatie-uitwisseling
	Onderzoek naar aard en omvang online fraude in het bedrijfsleven	Q3 2023	Werkgroep informatie-uitwisseling
Online platform voor kennisuitwisseling	Besluit tot ontwikkeling van een gemeenschappelijk online platform	Q2 2024	Werkgroep informatie-uitwisseling
	Eenduidige taxonomie	Q1 2023	Werkgroep informatie-uitwisseling

2. Gegevensdeling

Doelstelling

Om de effectiviteit van de aanpak van online fraude te kunnen verbeteren, is het belangrijk onderling (persoons-) gegevens van verdachten te kunnen delen met als doel om slachtofferschap te voorkomen. Uit de verkenning met alle partijen is duidelijk geworden dat dit momenteel als een van de grootste belemmeringen wordt ervaren voor een effectieve aanpak van online fraude. In het kader van de integrale aanpak worden mogelijkheden en problemen bij het (cross-sectoraal) delen van gegevens in kaart gebracht en geanalyseerd met als doel het vinden en creëren van mogelijkheden, door bijvoorbeeld het starten van pilots, om het delen van gegevens mogelijk te maken waar dat voor een effectieve aanpak van belang is.

Resultaat	Actie	Planning	Kerngroep/werkgroep/bijeenkomst
Inzicht in problematiek in geprioriteerde vraagstukken	Inventarisatie huidige mogelijkheden, kansen en knelpunten om keuze te kunnen maken welke vraagstukken geprioriteerd moeten worden aangepakt	Q1 2023	Werkgroep gegevensdeling
Oplossingsrichtingen voor knelpunten delen (persoons-) gegevens	Uitwerken oplossingsrichtingen op basis van best practices en casuistiek aangedragen door partners	Q3 2023	Werkgroep gegevensdeling
	Extern privacy advies over geanalyseerde oplossingsrichtingen	Q3 2023	Werkgroep gegevensdeling
	Uitwerken van oplossingsrichtingen in de praktijk in de vorm van pilots en op termijn borgen	Q2 2023	Werkgroep gegevensdeling
	Uitvoeren van de pilots 'suspicious devices' en 'checkfunctie 2.0'	Q3 2023	Werkgroep gegevensdeling
	Uitkomsten van de pilots omzetten naar praktijk	Afhankelijk van looptijd pilots	Werkgroep gegevensdeling
	Overleg met de Autoriteit Persoonsgegevens	Q2 2023	Werkgroep gegevensdeling
Informatie en advies voor partners	Opzetten van een expertteam voor een helpdesk	Q2 2023	Werkgroep gegevensdeling
	Onderzoek Juridische waarborgen bij gegevensdeling	Q2 2023	Werkgroep gegevensdeling

3. (Technische) barrières & interventies

Doelstelling

Het is van groot belang dat (technische) barrières en interventies, voor de meest voorkomende vormen van fraude, worden opgeworpen om burgers en bedrijven beter te beschermen, fraude te voorkomen en tegelijkertijd om het verdienmodel van criminele netwerken te verstoren. Hierbij is de inzet van o.a. fraude-, financiële en IT-experts essentieel om op basis van kennis en expertise tot concrete acties te kunnen komen.

Resultaat	Actie	Planning	Kerngroep/werkgroep/bijeenkomst
Analyse mogelijke (technische) barrières en interventies per fraudevorm	Besluit welke 2 fraudevormen eind Q1 geanalyseerd worden a.d.h.v. criminal journey/barrièremodel	Q1 2023	Werkgroep interventies
	Procesvoorstel opdracht uitwerking criminal journey/barrièremodel fraudevormen	Q1 2023	Werkgroep interventies
Mogelijkheden voor (technische) barrières en interventies geïdentificeerd	Gefaseerde analyse 5 meest voorkomende fraudevormen a.d.h.v. ‘criminal journey’ / ‘book of crimes’ / fraudecycli / ‘barrièremodel’	Q2 2023 Q4 2023	Werkgroep interventies
Informeren over ontwikkeling en toepassing nieuwe interventiemaatregelen	Inventarisatie nieuwe en door te ontwikkelen publiek en private technische interventies	Doorlopend	Werkgroep interventies
	Implementatie interventies, bestaande interventies breder inzetten en starten pilots (nieuwe) interventies	Doorlopend	Werkgroep interventies
	Monitoring effectiviteit van interventies	Doorlopend	Werkgroep interventies
	Verkennen ‘best practices’ en ‘lessons learned’ in andere landen	Doorlopend	Werkgroep interventies

4. Opvolging politie en openbaar ministerie

Doelstelling

De inzet van de politie en het openbaar ministerie (OM) is gericht op het realiseren van een brede, schaalbare en innovatieve aanpak, waarmee zowel de plegers als dienstverleners van online criminaliteit, waaronder online fraude, worden aangepakt. Naast opsporing en strafrechtelijke vervolging wordt ingezet op alternatieve interventies in samenwerking met publieke en private partners. Met deze brede bestrijding worden criminele activiteiten en netwerken verstoord, wordt strafbaar gedrag voorkomen, worden criminele winsten afgepakt en wordt opgetreden tegen strafbare feiten. Deze ambitie is geborgd in de Veiligheidsagenda 2023-2026.

Resultaat	Actie	Planning	Kerngroep/werkgroep/bijeenkomst
Inzicht effect en resultaten opsporing en vervolging	Periodiek informeren over ontwikkelingen en resultaten op het gebied van opsporing en vervolging	Doorlopend	Kerngroep
(Online) aangifteloket voor bedrijven en heldere afspraken over opvolging	Inrichting werkgroep met politie en bedrijfsleven	Q2 2023	Werkgroep Opsporing en vervolging
	Programma van eisen voor inrichten online aangifteloket	Q3 2023	Werkgroep Opsporing en vervolging
	Besluit tot uitvoeren verkenning inpassing in ICT-programma Politie	Q4 2023	Werkgroep Opsporing en vervolging
Landelijke implementatie van directe aansprakelijkheid naast strafrechtelijke afdoening	Presentatie plannen	Q1 2023	Kerngroep

5. Weerbaarheid/preventie

Doelstelling

De aanpak richt zich op het bewuster en weerbaarder maken van burgers en bedrijven om de werkwijzen die leiden tot online fraude tijdig te herkennen en (herhaald) slachtofferschap te voorkomen. Daarnaast richten we de aanpak ook op daderpreventie. Dit wordt bereikt door het breder inzetten van kansrijke bestaande initiatieven en een bredere uitrol van best practices. Waar nodig worden nieuwe campagnes en initiatieven ontwikkeld. Er wordt gestuurd op een betere afstemming en samenwerking op het gebied van communicatie en campagnes. Tenslotte wordt waar mogelijk en wenselijk aansluiting gezocht bij bestaande initiatieven en structuren.

Resultaat	Actie	Planning	Kerngroep/werkgroep/bijeenkomst
Afstemming communicatiemiddelen en planning	Inrichten breed overleg communicatieadviseurs	Q2 2023	Werkgroep weerbaarheid
	Afstemmen kernboodschap	Q2	Werkgroep weerbaarheid
	Opstellen campagnekalender	Q2	Werkgroep weerbaarheid
Brede aandacht voor het thema	Organisatie Week van de Veiligheid 2023 met onderdeel thema online fraude gericht op bedrijven en medewerkers	Q3 2023	Werkgroep weerbaarheid
	Aansluiten bij initiatieven zoals seniorenweek en verkennen op welke manier online fraude kan worden toegevoegd of vertaald binnen andere bestaande initiatieven zoals opleidingscurriculum mijn cyberrijbewijs, hackright, (Citydeals Cyber en Lokale weerbaarheid, geldezel projecten etc.	Doorlopend	Werkgroep weerbaarheid
	Organiseren 3 werkbezoeken bewindspersonen per jaar	Doorlopend	Werkgroep weerbaarheid
Beschikbaarheid preventieve campagnes en initiatieven om weerbaarheid te vergroten voor consumenten en bedrijven	Inventarisatie bestaande initiatieven en campagnes (ook op andere thema's) die in aanmerking komen voor 'bredere' uitrol	Q2 2023	Werkgroep weerbaarheid
	Start 3 interventies, die burgers en bedrijven weerbaarder maken, waaronder tegen 'social engineering'	Q4 2023	Werkgroep weerbaarheid

6. Hulp aan slachtoffers

Doelstelling

Slachtoffers (burgers en bedrijven) weten waar ze terecht kunnen, lezen wat ze zelf in eerste instantie kunnen doen, worden naar tevredenheid geholpen en ondersteund en de meldingsbereidheid van slachtoffers bij politie en hulpverlenende organisaties wordt vergroot. Hierbij wordt specifiek ingezet op een goede begeleiding (psychisch/technisch) van slachtoffers en het voorkomen van herhaald slachtofferschap.

Resultaat	Actie	Planning	Kerngroep/werkgroep/bijeenkomst
Inzicht in (slachtofferbeleving) bestaande meldpunten	Panelonderzoek naar slachtofferbeleving meldpunten	Q2 2023	Bijeenkomst
	Panelonderzoek slachtofferbeleving meldpunten	Q2 2023	Bijeenkomst
Inzicht in functioneren meldpunten	Inventarisatie bestaande meldpunten, samenwerking en onderlinge verwijzing	Q1 2023	Bijeenkomst
Meldpunten geven informatie over andere meldpunten	Opdracht voor opstellen factsheet o.g.v. inventarisatie	Q2 2023	Bijeenkomst
Meldpunten gaan verdergaand samenwerken	Opdracht voor onderzoek mogelijkheden samenwerking	Q2 2023	Kerngroep
Nieuwe meldpunten	Verkenning ‘phishing shield’	Q3 2023	Kerngroep
Bedrijven worden gezien als slachtoffer en krijgen passende hulp en ondersteuning	Voorstel haalbaarheidsonderzoek voor inrichting meldpunt voor bedrijven	Q4 2024	Kerngroep
Ondersteuningsaanbod aan kwetsbare groepen en herhaalde slachtoffers van online fraude	Voorstel voor een project om slachtoffers aanbod te doen om hun ‘beveiliging’ op orde te brengen m.b.t. gedrag (cursus) en techniek (beveiliging)	Q3 2023	Bijeenkomst

Dit is een uitgave van:

Ministerie van Justitie en Veiligheid

Februari 2023