



CCV centrum voor
criminaliteitspreventie en
veiligheid

Echt of nep? Cyberweerbaarheid voor senioren

Handleiding interactieve film

Versie 3.0
Februari 2025

VAR VeiligheidsAlliantie
regio Rotterdam

1 Inleiding

Steeds meer mensen worden het slachtoffer van digitale criminaliteit via de computer, het internet, de telefoon of een app. Vaak zijn ouderen hier de dupe van. Het is dan ook belangrijk dat zij weerbaarder worden tegen digitale criminaliteit.

Versterken cyberweerbaarheid senioren

Daarom is er speciaal voor ouderen de interactieve film *Echt of Nep? Cyberweerbaarheid voor senioren* gemaakt. Met deze film kun je senioren op een laagdrempelige manier kennis bijbrengen over veilig internetgebruik. Niet door informatie te zenden, maar door ze aan de hand van vijf praktijksituaties mee te nemen en ze na te laten denken over de keuzes die gemaakt kunnen worden.

Met deze interactieve film kunnen bijvoorbeeld gemeenten, buurthuizen, verenigingen voor ouderen, welzijnswerk, politie, bibliotheken het gesprek aangaan met senioren over hun ervaringen met digitale criminaliteit en hen meer leren over veilig internetgebruik.

Interactieve film

De interactieve film is een PowerPointpresentatie met vijf filmpjes over verschillende vormen van digitale criminaliteit. Deze zijn: hulpvraagfraude/WhatsAppfraude, phishing, helpdeskfraude, spoofing en datingfraude.

Elke vorm van digitale criminaliteit ofwel delict wordt behandeld in een apart filmpje. Per delict zijn steeds drie scènes opgenomen. De presentatie geeft je keuzemogelijkheden. Na elke scène wordt het filmpje stopgezet en wordt aan de senioren gevraagd wat zij in deze situatie zouden doen. De film gaat dan verder met de keuze die gemaakt wordt. Op deze manier ervaren senioren zelf wat er gebeurt, ook als er een verkeerde keuze wordt gemaakt. Zo blijft de opgedane kennis beter hangen.

Film opvragen

De film is gratis online beschikbaar op [de website van het CCV](#). Er is ook een downloadbare PowerPoint beschikbaar. Deze is gratis op te vragen door te mailen aan: tom.weijers@hetccv.nl.

Inhoud handleiding

In deze handleiding vind je alles wat je moet weten over het organiseren van een bijeenkomst voor senioren en het gebruik van de film om de weerbaarheid van ouderen te versterken:

- Het organiseren van een bijeenkomst (pagina 3)
- Tijdens de bijeenkomst (pagina 5)
- Het gesprek met de zaal (pagina 6)
- Hoe werkt de film? (pagina 8)

Ook vind je in de bijlagen enkele hulpmiddelen die je helpen bij het organiseren en houden van de bijeenkomst:

- Voorbeeldtekst uitnodiging bijeenkomst (pagina 14)
- Checklist organiseren bijeenkomst (pagina 15)
- Notities voor ieder delict (pagina 16 t/m 23)
- Informatieblad online criminaliteit (pagina 24)
- Factsheet informatiepunten en aangiften digitale criminaliteit (pagina 25)

2 Organisatie bijeenkomst

Ga jij een bijeenkomst organiseren voor senioren waarbij de interactieve film *Echt of Nep? Cyberweerbaarheid voor senioren* wordt gebruikt? Dan vind je hier alle informatie die je nodig hebt.

Uitnodiging

Als organisator zorg je ervoor dat de bijeenkomst bekend is bij de mensen die je wilt uitnodigen. Hiervoor stel je een uitnodiging op. Daarin staat voor wie de bijeenkomst is en waar en wanneer deze plaatsvindt. In de bijlage (pagina 14) vind je een voorbeeldtekst voor de uitnodiging.

De uitnodiging kun je verspreiden via flyers, affiches, lokale media en social media. Vraag aan andere organisaties zoals de gemeente, de bibliotheek, het buurthuis, ouderenbond of zij je willen helpen met het verspreiden van de uitnodiging.

Locatie

Zorg voor een locatie die goed bereikbaar is en een goede akoestiek heeft zodat iedereen alles goed kan horen. Let hierbij op de volgende dingen:

- Is de locatie rolstoelvriendelijk?
- Is er ringleiding voor slechthorenden?
- Heeft de locatie een microfoon, een loopmicrofoon, beamer en groot scherm?
- Is de locatie groot genoeg zodat iedereen kan zitten?
- Is er genoeg ruimte om halverwege de bijeenkomst een pauze te houden?
- Hebben ze koffie en thee voor de mensen die komen?

Richt de zaal in met tafels en stoelen die richting het podium of de spreker staan. Zet bij de uitgang een tafel met voorlichtingsmateriaal om na afloop mee te geven. In de bijlage vind je een informatieblad over online criminaliteit. Ook vind je daar een blad met informatie over organisaties waar mensen met vragen naartoe kunnen. Print deze uit en leg ze op de tafel.

Zorg voor voldoende koffie, thee en wat lekkers als de mensen binnenkomen en tijdens de pauze. Zet eventueel ook wat fris of water neer.

Programma

De bijeenkomst zelf duurt ongeveer 1,5 uur. Dit is wel sterk afhankelijk van het gesprek met de deelnemers. Soms ben je sneller klaar en soms duurt een bijeenkomst wat langer.

Het is belangrijk dat je tijd maakt voor inloop, een pauze en om na afloop nog na te praten. Dan hebben mensen de ruimte om met elkaar te praten en hun ervaringen delen. Ook kunnen zij met hun verhalen en hun vragen komen naar degene die de bijeenkomst leidt.

Het programma kan je zelf invullen. Er zijn in totaal 8 filmpjes. Dit zijn er erg veel voor één bijeenkomst. We raden daarom aan om 4 á 5 filmpjes te kiezen voor een bijeenkomst. Een bijeenkomst kan je bijvoorbeeld zo invullen:

- Inloop (30 minuten)
- Welkom (10 minuten)
- Twee filmpjes (30 minuten)
- Pauze (20 minuten)
- Twee of drie filmpjes (30 minuten).
- Na afloop van de bijeenkomst nog napraten (30 minuten)

Dingen die je nodig hebt

De film kan online of via een PowerPointbestand afgespeeld worden. Voor het afspelen van de film heb je een laptop nodig. Voor de online versie heb je een internetverbinding nodig en voor de PowerPoint moet je het PowerPointbestand gedownload hebben. Daarnaast heb je een beamer en groot scherm nodig. Deze verbind je met de laptop zodat op het grote scherm de presentatie komt te staan. Zorg tenslotte ook dat het geluid van de filmpjes goed te horen is.

Zorg dat je laptop een HDMI-aansluiting heeft, of zorg voor een verloopstukje dat in je laptop past en een HDMI-aansluiting bevat.

Het kan ook handig zijn om microfoons te gebruiken. Gebruik dan twee microfoons: een microfoon voor de presentator en een loopmicrofoon voor de reacties uit de zaal. Bij een grote zaal is het handig om twee loopmicrofoons te hebben.

Mensen die je nodig hebt

Tijdens de bijeenkomst heb je twee personen nodig: de presentator en de ondersteuner.

Presentator

Iedereen die enthousiast is en zich comfortabel voelt om met mensen in gesprek te gaan over digitale criminaliteit, kan de interactieve film presenteren. Je kunt als organisator de film zelf presenteren, of je vraagt iemand anders. Bijvoorbeeld van je eigen organisatie, van de politie, ouderenwerk, buurthuis of de bibliotheek.

De presentator praat de bijeenkomst aan elkaar. Hij of zij gaat ook in gesprek met de deelnemers: waarom denken ze dat dit het juiste antwoord is? Hebben ze zelf weleens zoiets meegemaakt?

Ondersteuner

De ondersteuner helpt bij de organisatie van de bijeenkomst. Hij of zij zet alles klaar, ontvangt de deelnemers, loopt tijdens de bijeenkomst met de loopmicrofoon door de zaal en houdt de tijd in de gaten.

Kennis over digitale criminaliteit

Zorg ervoor dat iemand aanwezig is met kennis over digitale criminaliteit die inhoudelijke vragen kan beantwoorden over digitale criminaliteit of het doen van aangifte.

Dit kan de presentator of ondersteuner zelf zijn. Mochten deze personen niet genoeg kennis hebben over digitale criminaliteit, nodig dan een aanvullend persoon uit. Dit kan een wijkagent of iemand van je gemeente zijn die zich bezighoudt met het onderwerp.

Checklist

In de bijlage (pagina 15) vind je een checklist met een overzicht van wat je moet organiseren voor een bijeenkomst.

3 Tijdens de bijeenkomst

Hieronder lees je wat de presentator kan doen tijdens de bijeenkomst en waar hij of zij op moet letten.

Vorbereiding

Als je de presentator bent, zorg dan dat je weet hoe je de film moet afspelen en wat je moet vertellen bij ieder filmpje. Je leest alles over het afspelen van de film op pagina 8. In de PowerPoint presentatie zit een instinker. Wees je hier bewust van. Hier lees je meer over in hoofdstuk 5: Hoe werkt de film.

Print de notities in de bijlage op pagina 16 t/m 23 uit, zodat je deze bij de hand kunt houden tijdens de presentatie.

Bovendien is het goed om een keer te oefenen en om de presentatie eerst voor jezelf door te nemen.

Welkom en start

Wanneer de bijeenkomst start, heet je iedereen welkom en leg je het doel uit.

Vertel dat het fijn is dat iedereen tegenwoordig veel dingen kan regelen via de telefoon of computer. Maar, er zijn ook criminelen zijn die hier misbruik van maken. In deze bijeenkomst leren de deelnemers hoe zij digitale oplichting kunnen proberen te voorkomen.

Leg uit dat de deelnemers een aantal korte filmpjes te zien krijgen. Je vraagt de deelnemers zich te verplaatsen in de acteur.

Afspelen filmpjes

Hierna start je de eerste scène. Aan het eind van de scène stopt het filmpje. Je gaat nu in gesprek met de deelnemers. Wat hebben ze gezien?

De presentatie geeft je nu een keuzemogelijkheid: reageren of negeren? Je vraagt wat de deelnemers zouden doen. Je telt het aantal handen voor reageren en voor negeren. Het antwoord met de meeste stemmen wordt gekozen om te tonen aan de zaal. Je klikt daarom op het gekozen filmpje, waarna deze scene wordt afgespeeld. Zodra de scène is afgelopen, praat je er weer over met de zaal. Zorg ervoor dat deelnemers de ruimte krijgen om te vertellen over hun eigen ervaringen. Vraag bijvoorbeeld of iemand de situatie herkent of ooit heeft meegemaakt.

Laat ook de keuze van de minderheid van de deelnemers zien. Wat gebeurt er dan? Leg uit waarom het ene antwoord goed is en het andere fout.

Belangrijke punten:

- Zorg steeds voor interactie met de zaal. Wat zou iemand doen? Heeft iemand dit een keer meegemaakt?
- Laat ook ruimte voor het vertellen van iemands ervaringen. Deelnemers vinden het heel fijn om te merken dat ze niet de enige zijn en leren veel van elkaars verhalen.
- Geef aan dat het internet niet eng is en juist heel handig. Er zijn risico's, maar geen directe gevaren.
- Benadruk dat mensen zich niet hoeven te schamen als ze slachtoffer zijn geworden. Dit is niet dom en kan iedereen overkomen. Dring bij het slachtoffer aan om hier aangifte van te doen.

4 Het gesprek met de zaal begeleiden

Als presentator voer je tijdens de bijeenkomst een gesprek met de zaal. Je leest hier hoe je dat doet.

Veilige sfeer creëren

Probeer een veilige sfeer te creëren. Een veilige sfeer is nodig zodat deelnemers hun eigen ervaringen met de zaal durven delen. Je kunt als presentator een veilige sfeer creëren door met de deelnemers een aantal afspraken te maken met elkaar.

Geef bij begin van de bijeenkomst aan:

- We laten elkaar uitpraten. En praten niet door het verhaal van een ander heen.
- We zijn respectvol naar elkaar. En lachen elkaar niet uit en oordelen niet.
- We respecteren elkaars privacy en delen de verhalen niet met anderen.
- We spreken vanuit onszelf, niet over algemeenheden ('ik maak mee dat' i.p.v. 'men zegt').

Stimuleren gesprek

Als je merkt dat het gesprek met de zaal niet of langzaam op gang komt, dan kun je dit stimuleren door vragen te stellen zoals:

- Wie herkent deze situatie?
- Wie is zelf weleens slachtoffer geweest van digitale oplichting en wil zijn of haar verhaal met de zaal delen?
- Wie kent iemand die dit weleens heeft meegemaakt of weleens slachtoffer is geworden van digitale criminaliteit?

Aanvullende vragen zijn:

- Wil iemand daar iets aan toevoegen?
- Kun je daar iets over vertellen?
- Wie wil daar nog meer over vertellen?
- Hoe is dat voor anderen?
- Wat roept dit bij jullie op?
- Wie kan zich dat wel voorstellen?

Voorbeelden van ingewikkelde situaties

Soms kunnen ingewikkelde situaties ontstaan tijdens een gesprek. Hier volgen een aantal van deze situaties en hoe je ermee om kunt gaan:

Wat doe je als...

... iemand voortdurend aan het woord is en geen ruimte laat voor anderen?

- Je kunt vriendelijk de bijdrage van die persoon kort samenvatten ("Je zegt dus als ik het goed begrijp dat je...") en hem of haar bedanken voor de bijdrage.
- Van daaruit maak je de overgang naar de bijdrage van een ander. Bijvoorbeeld door te informeren: "Herkent iemand anders dit ook?"

... iemand heel erg lang aan het woord is?

- Je vraagt die persoon om 'met het oog op de tijd' zijn of haar vraag of bijdrage af te ronden. Andere deelnemers moeten immers ook aan bod kunnen komen.

... een deelnemer emotioneel wordt of een heftige ervaring deelt?

- Stel de persoon op het gemak door bijvoorbeeld te zeggen dat je zijn of haar emotie of situatie begrijpt.
- Vraag de persoon of hij of zij iets nodig heeft om de bijeenkomst voort te zetten, zoals wat drinken, een frisse neus halen of met iemand één op één praten.

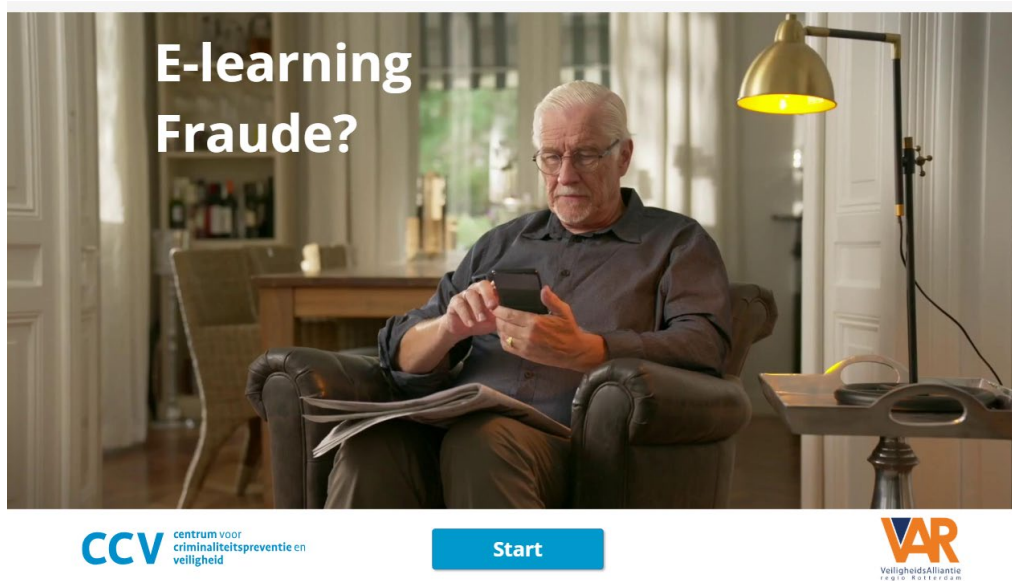
- Ook kun je nazorg bieden, bijvoorbeeld door na afloop van het gesprek bij de persoon te checken hoe het gaat.
- Verwijs iemand naar de wijkagent of naar een andere instantie die meer kan vertellen over de mogelijke oplossingen voor de vervelende ervaring waarmee de persoon te maken heeft gehad.

5 Hoe werkt de film?

Hier lees je stap voor stap hoe het PowerPoint-bestand werkt en hoe je de film kunt afspelen. De plaatjes komen van de online versie. De knoppen werken hetzelfde in de PowerPoint. Ze kunnen er wel iets anders uit zien.

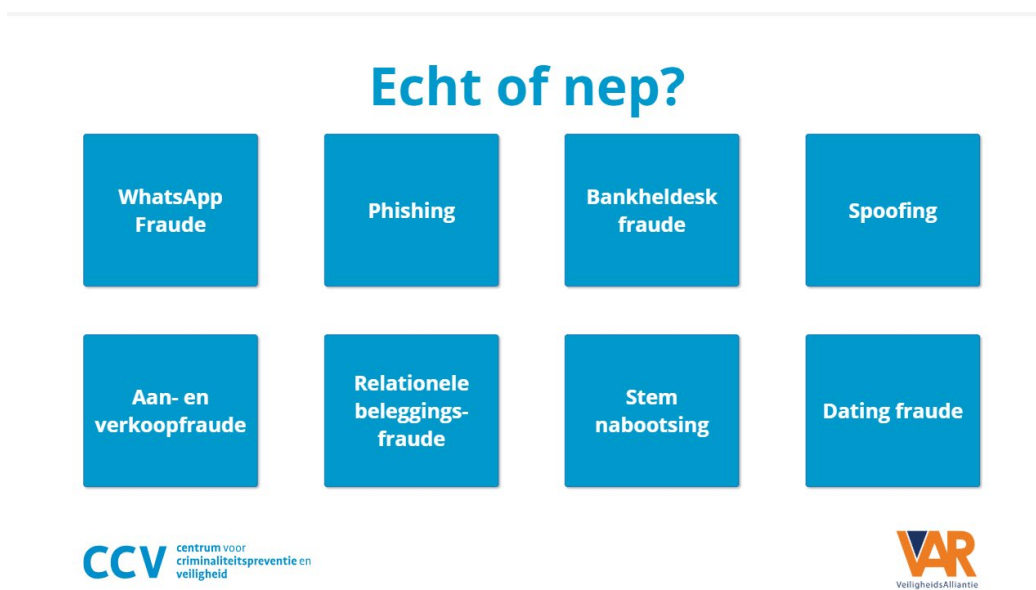
Stap 0 (alleen voor de online versie)

Na het openen van de online versie via de website van het CCV zie je een startscherm. Klik op start en je kan beginnen.



Stap 1

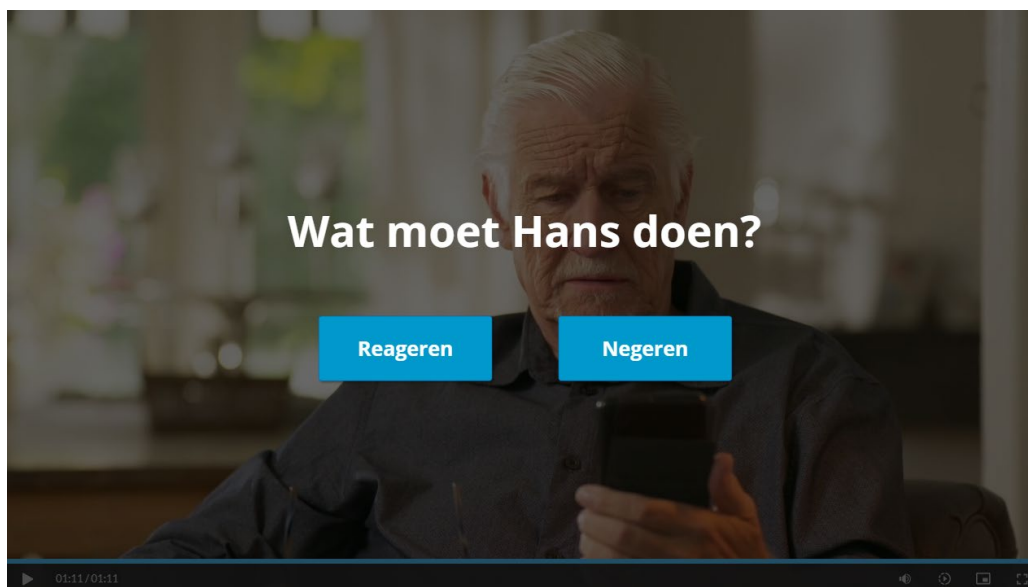
Voor de online versie: Na het klikken op start krijg je het overzicht te zien van de acht delicten.
Voor de PowerPoint: Eerst start je PowerPoint op en open je het PowerPointbestand 'Echt of Nep 2025.pptx'. In PowerPoint kies je nu voor 'afspelen vanaf het begin'. Je krijgt dan een overzicht van de acht delicten.



Kies het delict dat je wil laten zien door op die knop te klikken. Na het doorlopen van dit deel van de presentatie, kom je automatisch weer terug op het beginscherm. Kies dan voor het volgende delict.

Stap 2

Nadat je op de knop 'WhatsApp-fraude' (of een ander delict) hebt geklikt, start automatisch de eerste video. De video's duren tussen de 30 en 90 seconden. Als de video is afgespeeld, verschijnt automatisch het eerste keuzeschermb.



Overleg met de zaal wat de acteur (Hans) moet doen: reageren of negeren. Overweeg met de deelnemers beide opties. Als de zaal een keuze heeft gemaakt klik je op 'reageren' of 'negeren'. Automatisch wordt het volgende filmpje afgespeeld.

Stap 3

Na het afspelen verschijnt er weer een keuzeschermb. Met dat keuzeschermb laat je de zaal ook kennismaken met 'de andere' keuze. In het voorbeeld hieronder is dat 'negeren'. Klik op 'negeren' en zie wat er zou zijn gebeurd als de deelnemers hiervoor hadden gekozen.



Stap 4 (alleen voor de PowerPoint)

Let op: nu volgt een instinker!

Na het bekijken van 'de andere keuze' (in dit voorbeeld 'negeren'), kom je automatisch weer terug op een keuzescherf. Op dit scherm krijg je de mogelijkheid om nog een keer het andere filmpje te bekijken (in dit voorbeeld 'reageren'). **Doe dit niet, klik op overslaan!** In de online versie van de film komt dit probleem niet voor.

WhatsApp-fraude

Wat zou er zijn gebeurd als Hans voor 'reageren' had gekozen?

Reageren

Overslaan

Je kunt elk filmpje namelijk **maar 1 keer afspelen**. Als je per ongeluk toch op de knop klikt, dan verschijnt wel het eerste beeld van het filmpje, maar begint deze niet automatisch af te spelen. De PowerPointpresentatie kan dan vastlopen.

Als dit je toch overkomt, sluit dan de PowerPointpresentatie af en start deze opnieuw op. Via de thumbnails aan de linkerkant van de PowerPoint kun je direct door naar de dia waar je was gebleven en vanaf dit punt verder gaan met afspelen.

Stap 5

Wanneer je door de drie keuzes heen bent, volgen er nog twee dia's. Op de eerste dia staat een korte tekstuele omschrijving van het delict. In dit voorbeeld is dat 'Wat is WhatsApp fraude nu eigenlijk?'

In de notities (zie bijlage 16 t/m 23) vind je voor ieder delict een bredere uitleg. Deze kun je bij je presentatie gebruiken.

WhatsApp-fraude

Criminelen doen zich via tekstberichten voor als een goede bekende die u vraagt om geld of iets te betalen.



Tips



Na de uitleg over het delict, klik je op tips. Je gaat dan naar de volgende dia.

Stap 6

Op de dia staan de drie belangrijkste tips (voorbeeld: zie afbeelding 6). In de notities vind je voor ieder delict nog meer tips. Bespreek de tips met de zaal.

WhatsApp-fraude

- Meld WhatsApp-fraude zo snel mogelijk bij uw bank
- Wees altijd alert als om geld wordt gevraagd, ook bij een bekend telefoonnummer.
- Bel altijd eerst de persoon zelf op het voor u bekende nummer. Niet gebeld = geen geld.



Menu



Stap 7

Als het onderwerp is afgesloten, klik je op 'Menu'. Je komt dan weer op het beginscherm met een overzicht van de acht delicten. Kies dan voor het volgende delict.

Echt of nep?



Alle andere vormen van digitale criminaliteit zijn op dezelfde manier opgebouwd als het voorbeeld van WhatsApp-fraude.

Notities

Extra informatie over elk van de delicten kan je vinden in de bijlagen (pagina 16 t/m 23). Gebruik deze notities tijdens de presentatie als extra ondersteuning.

Bijlagen met hulpmiddelen

- Voorbeeldtekst uitnodiging bijeenkomst (pagina 14)
- Checklist organiseren bijeenkomst (pagina 15)
- Notitie Hulpvraagfraude / WhatsApp fraude (pagina 16)
- Notitie Phishing (pagina 17)
- Notitie Helpdeskfraude (pagina 18)
- Notitie Spoofing (pagina 19)
- Notitie Datingfraude (pagina 20)
- Notitie aan- en verkoopfraude (pagina 21)
- Notitie relationele beleggingsfraude (pagina 22)
- Notitie stem nabootsing (pagina 23)
- Informatieblad online criminaliteit (pagina 24)
- Factsheet informatiepunten en aangiften digitale criminaliteit (pagina 25)

Voorbeeldtekst uitnodiging

Echt of Nep? Een bijeenkomst voor senioren over digitale oplichting

Krijgt u weleens een mail of bericht dat u niet vertrouwt of waarvan u denkt, klopt dit wel? In deze tijd gaat alles snel en doen we veel via internet. Criminelen maken hier misbruik van. Ze proberen u bijvoorbeeld op te lichten of geld van u te stelen.

Daarom organiseert XXX op XXX de bijeenkomst *Echt of Nep?* Deze bijeenkomst is voor senioren en is gratis. De bijeenkomst is bedoeld om mensen weerbaarder te maken tegen digitale oplichting via de computer, het internet, de telefoon of een app. Aan de hand van korte filmpjes praten we over digitale oplichting. Ook krijgt u handige tips over onder andere nep e-mails en nep-appjes.

Wij zien u graag op deze bijeenkomst en zorgen voor koffie en thee met wat lekkers.

Waar en wanneer?

Datum: XXX

Tijd: XXX

Locatie: XXX

Aanmelden

Wilt u erbij zijn? Meld u dan aan via XXX.

Checklist bijeenkomst

Wat moet je regelen voor een bijeenkomst Echt of Nep?

- ☐ Voor de online versie: een goede internetverbinding
Voor de PowerPoint: het PowerPointbestand gedownload op de laptop
- ☐ Een locatie die groot genoeg is, goed bereikbaar is voor ouderen en goede akoestiek heeft. Liefst met ringleiding
- ☐ Uitnodiging, breed verspreid met hulp van andere organisaties
- ☐ Laptop met aansluiting voor beamer
- ☐ Beamer, groot scherm, microfoon en loopmicrofoon (1 of 2)
- ☐ Een presentator
- ☐ Een ondersteuner
- ☐ Indien nodig: iemand met kennis over digitale criminaliteit
- ☐ Voldoende tafels en stoelen, gericht naar spreker
- ☐ Tafel bij uitgang voor informatiemateriaal
- ☐ Koffie, thee en iets lekkers
- ☐ Uitgeprinte informatiebladen voor alle deelnemers (bijlage handleiding)
- ☐ Uitgeprinte factsheet voor alle deelnemers (bijlage handleiding)
- ☐ Voor presentator: notities vijf delicten (bijlage handleiding)

Notitie Hulpvraagfraude/ WhatsApp fraude

Wat is Hulpvraagfraude/WhatsApp-fraude?

Tekst op de dia

Criminelen doen zich via tekstberichten voor als een goede bekende die je vraagt om geld of iets te betalen.

Extra informatie

Via apps communiceren we tegenwoordig veel met elkaar. Denk bijvoorbeeld aan WhatsApp of sms. Oplichters kunnen hier misbruik van maken. Ze proberen geld af te troggelen door zich voor te doen als een bekende. Bij hulpvraagfraude via WhatsApp of sms ontvangt iemand een bericht van een oplichter die zich voordoet als bijvoorbeeld je (klein)zoon, (klein)dochter, vriend of vriendin. Vaak begint het met een berichtje dat de bekende een nieuw telefoonnummer heeft. Daarna krijg je al snel een bericht dat diegene in de problemen zit en geld nodig heeft. De crimineel vraagt je dan om te helpen door middel van een betaalverzoek.

Tips (wat kun jezelf doen)?

- Meld WhatsApp-fraude zo snel mogelijk bij je bank
- Wees altijd alert als om geld wordt gevraagd, ook bij een bekend telefoonnummer.
- Bel altijd eerst de persoon op het voor jou bekende nummer. Niet gebeld = geen geld.
- Doe altijd aangifte bij de politie (ook bij een poging).
- Controleer het rekeningnummer dat de oplichter opgeeft. Komt het overeen met het rekeningnummer van je bekende?
- Scherm je social media af. Het gaat niet alleen om je telefoonnummer, maar ook om foto's die je openbaar hebt staan en de relaties die je op jouw sociale media hebt staan (bijvoorbeeld 'vader van' of 'getrouwd met').
- Je kunt ook melding doen van een poging tot WhatsApp-fraude bij de fraudehelpdesk <https://www.fraudehelpdesk.nl/>.



Notitie Phishing

Wat is Phishing?

Tekst op de dia

Bij Phishing proberen criminelen je door e-mails naar een valse website te lokken. Daar stelen ze je gegevens of geld.

Extra informatie

Bij Phishing 'vissen' fraudeurs aan de telefoon of via valse berichten of brieven naar vertrouwelijke informatie. Denk bijvoorbeeld aan bankgegevens en persoonsgegevens zoals je BSN en wachtwoorden voor digitaal betalen en bankieren. Ze kunnen ook direct een betaalverzoek sturen, bijvoorbeeld via een nep-Tikkie. Met de gegevens die je daar invult, kunnen internetcriminelen je vervolgens veel geld afhandig maken.

Tips (wat kun je zelf doen)?

- Gaat het om geld en is er haast bij? Vertrouw dit niet. Eerst checken dan klikken.
- Klik nooit op een link van een mail die je niet vertrouwt en download geen bijlagen.
- Bij twijfel, bel de organisatie waar het over gaat en doe altijd aangifte bij de politie.
- Betaal niet zomaar, maar controleer altijd eerst of alles klopt, door de afzender en link te controleren op betrouwbaarheid.
- Gebruik nooit het telefoonnummer uit de e-mail, deze kan nep zijn.
- Doe altijd aangifte bij de politie als je opgelicht bent.
- Je kunt ook melding doen van een poging tot Phishing bij de fraudehelpdesk
<https://www.fraudehelpdesk.nl/>



Notitie Helpdeskfraude

Wat is Helpdeskfraude?

Tekst op de dia

Bij helpdeskfraude doen internetcriminelen alsof ze helpdeskmedewerkers van grote, bekende bedrijven zijn.

Extra informatie

Bij helpdeskfraude word je meestal zomaar gebeld door iemand die zich voordoet als medewerker van bijvoorbeeld een bank. De oplichter zegt dat er wat mis is met je betaalrekening of bankaccount en biedt aan om te helpen. Hij of zij vraagt je om geld over te maken naar een zogenaamde kluisrekening of veilige rekening. Ook kan de oplichter vragen om privé-gegevens of inloggegevens.

Tips (wat kun jezelf doen)?

- Veilige kluisrekeningen bestaan niet. Zoek het echte nummer van de bank op en bel zelf.
- Meld helpdeskfraude altijd bij het echte bedrijf en doe altijd aangifte bij de politie.
- Een bankmedewerker haalt nooit bij je thuis je bankpas of pincodes op en vraagt je ook niet om deze zelf op te sturen. Ga hier dus niet in mee.
- Banken vragen nooit om geld over te maken naar een andere rekening.
- Banken vragen nooit om persoonlijke gegevens. Verbreek de verbinding als je het niet vertrouwt.
- Zoek zelf het telefoonnummer op van de instantie of bank en doe navraag.
- Je kunt ook melding doen van een poging bij de fraudehelpdesk <https://www.fraudehelpdesk.nl/>.



Notitie Spoofing

Wat is Spoofing?

Tekst in beeld

Bij spoofing gebruiken internetcriminelen een identiteit, emailadres of telefoonnummer dat (bijna) hetzelfde is als het origineel.

Extra informatie

Bij spoofing nemen internetcriminelen een andere identiteit aan. De crimineel doet zich voor als een bank, verzekeringsmaatschappij, overheidsinstantie, kennis of goede bekende. Zo probeert de crimineel achter je persoonsgegevens of je pincode te komen, malware op je computer te plaatsen of je direct geld afhandig te maken. Soms manipuleert de oplichter het telefoonnummer, waardoor ook daadwerkelijk het telefoonnummer van de instantie op uw telefoon verschijnt.

Tips (wat kun jezelf doen)?

- Gaat het om geld en is er haast bij? Vertrouw dit niet. Eerst checken dan klikken.
- Klik nooit op een link die u niet vertrouwt en download geen bijlage.
- Zoek zelf het telefoonnummer op van de instantie en doe navraag.
- Betaal niet zomaar en deel geen gegevens, maar controleer altijd eerst of alles klopt, door de afzender en link te controleren op betrouwbaarheid.
- Word je gebeld door een medewerker die zegt voor een bank of overheidsinstantie te werken? Stel veel vragen en zeg dat je zijn of haar identiteit wilt bevestigen.
- Hang op en zoek het telefoonnummer op van de organisatie, en bel op die manier terug. Zo weet je zeker dat u echt iemand van deze organisatie aan de lijn hebt.
- Maak nooit zomaar geld over, klik nooit zomaar op links en stuur nooit je pinpas op.
- Doe altijd aangifte bij de politie als je opgelicht bent.
- Je kunt ook melding doen van een poging bij de fraudehelpdesk <https://www.fraudehelpdesk.nl/>



Notitie Datingfraude

Wat is datingfraude?

Tekst in beeld

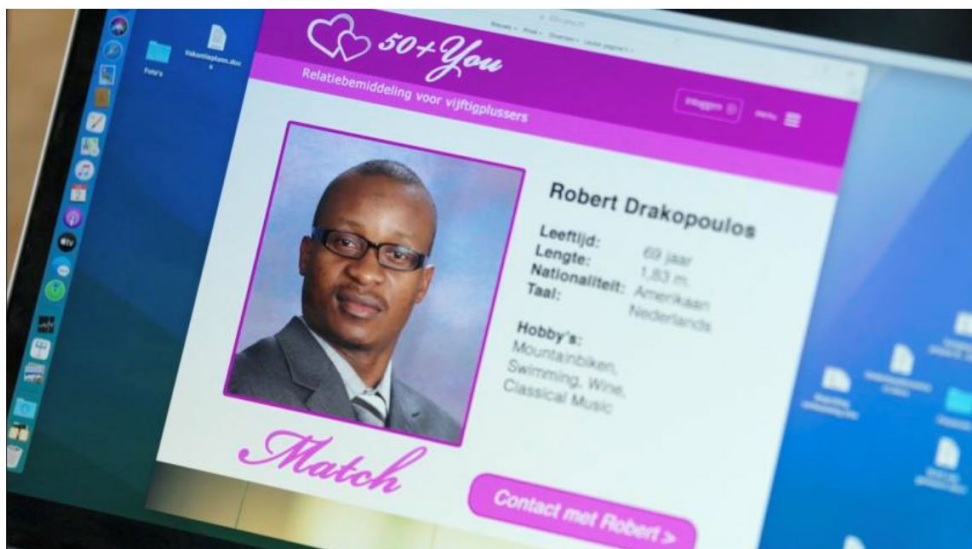
Bij datingfraude word je opgelicht door iemand die je hebt leren kennen via een datingsite, website of sociale media.

Extra informatie

Bij datingfraude wordt er via een datingwebsite of -app contact gelegd met het potentiële slachtoffer. Hij of zij kweekt een vertrouwensband met je en vraagt je om te communiceren via WhatsApp of e-mail. Vervolgens vraagt hij of zij met een smoes om geld. Bijvoorbeeld een (financieel) noodgeval of om elkaar te ontmoeten.

Tips (wat kun jezelf doen)?

- Maak nooit geld over naar iemand die je nog nooit in het echt hebt ontmoet.
- Controleer de foto van het datingprofiel via Google Image of TinEye.
- Blijf communiceren via de datingwebsite en niet via e-mail of WhatsApp.
- De fraudeur probeert de datingpartner te isoleren om hem/haar makkelijker te beïnvloeden. Houd altijd familie en vrienden op de hoogte.
- Doe altijd aangifte bij de politie als je opgelicht bent.
- Je kunt ook melding doen van een poging bij de fraudehelpdesk <https://www.fraudehelpdesk.nl/>



Notitie Aan- en Verkoopfraude

Wat is aan- en verkoopfraude?

Tekst in beeld

Bij aankoopfraude maak je geld over naar een persoon of bedrijf zonder de dienst of het product te ontvangen waarvoor is betaald. Bij verkoopfraude worden goederen wel geleverd, maar betaalt de ontvanger daar niet voor.

Extra informatie

Binnen de online aan- en verkoopfraude maken we onderscheid tussen handelsplaatsen (zoals Marktplaats en webwinkels). Sommige valse webwinkels zijn exacte kopieën van bestaande webwinkels. De politie geeft aan dat mensen vaak bij een malafide webwinkel komen via sociale media. Voornamelijk via Instagram. Maar ook via andere soorten sociale media. Facebook is in trek bij deze doelgroep.

Tips (wat kun jezelf doen)?

- Controleer de verkoper op meldingen bij de politie en bij veiliginternetten. [Check de \(ver\)koper | politie.nl](#) en [ScamCheck \(veiliginternetten.nl\)](#). Let op: geen melding betekent niet dat u geen risico loopt.
- Controleer betaalmogelijkheden bij een website. Is het mogelijk om met creditcard te betalen of achteraf? Met een creditcard kan je je geld terugkrijgen en bij achteraf betalen betaal je pas als je het product hebt.
- Bekijk de beoordelingen van een webshop. [Trustpilot](#) is een handige website om te controleren wat voor beoordelingen een webshop heeft.
- Kijk hoe lang een verkoper actief is bij een onlinehandelssite. Dit is voornamelijk handig voor handelssites waar particulieren actief zijn zoals marktplaats
- Stuur de (ver)koper nooit een kopie van uw legitimatiebewijs!
- [Tips om veilig te handelen op het internet | politie.nl](#)
- Doe aan prijsvergelijking: is de gevraagde prijs reëel? Als iets te mooi is om waar te zijn, dan is dat meestal ook zo.



Notitie Relationale beleggingsfraude (pig butchering)

Tekst in beeld

Bij 'relationele beleggingsfraude' worden mensen verleid om te investeren in cryptomunten, zoals Bitcoin. De oplichter doet zich voor als iemand met een luxe levensstijl, om daarmee te laten zien dat dit voor jou ook mogelijk is. Ze willen jou laten zien hoe je ook snel rijk kan worden.

Extra informatie

Bij 'relationele beleggingsfraude' manipuleren cybercriminelen hun slachtoffer net zolang tot ze een vertrouwensband of zelfs liefdesband hebben opgebouwd. Dit is soms een lang proces waarin echt langzaam aan de relatie wordt gewerkt. Door de tijdsspan is het slachtoffer bereid om een duizenden of honderdduizenden euro's over te maken. Het slachtoffer wordt eerst "vetgemest" met een klein financieel succesje en liefdevolle berichten. De oplichter laat het slachtoffer succesvolle investeringen zien en overtuigt het slachtoffer dat iedereen dit kan. De politie en het OM noemt dit Pig Butchering.

Tips (wat kun jezelf doen)?

- (Signaal) Degene met wie je praat, woont in een ander land of ver van je vandaan.
- Degene met wie je praat, heeft altijd smoesjes om je niet persoonlijk te ontmoeten. Probeer dus altijd persoonlijk af te spreken. Als dit niet kan, zou er een alarmbel af moeten gaan.
- Onderteken nooit zomaar een (smart)contract. Online ondertekenen is akkoord gaan dmv een vingerafdruk, gezichtsherkenning of een wachtwoord invoeren.
- Deel met de omgeving dat U iemand online heeft ontmoet. Uw omgeving kan dan kritisch meekijken. Een oplichter probeert u hiervan te weerhouden.
- Degene waarmee u praat dringt aan op het investeren, vraagt je om geld of om persoonlijke (bank) gegevens.
- Let op: als iemand slachtoffer is geworden waarbij er crypto is gestolen. Kan het zijn dat het slachtoffer zoek naar online hulp om het geld terug te halen. Hiervoor wordt dan betaald en er wordt niets geleverd. Dit noemen we recovery scams.
- Degene met wie je praat geef je extreem veel aandacht, complimenten en (soms) cadeautjes, dit heet 'lovebombing'.



Notitie AI stem nabootsing (AI Voice Cloning)

Tekst in beeld

Voice cloning is een geavanceerde technologie waarmee iemands stem nauwkeurig kan worden gereproduceerd met behulp van kunstmatige intelligentie. Dit betekent dat iemand anders jouw stem kan nabootsen, inclusief de toon, het ritme en de intonatie.

Extra informatie

Voice cloning kan ook ingezet worden voor meer schadelijke doeleinden. Zo kan het als hulpmiddel worden gebruikt voor oplichting en fraude. Een gekloonde stem van een bekende kan bijvoorbeeld worden gebruikt om een slachtoffer telefonisch te vragen om geld over te maken. Het zonder toestemming opnemen en kunstmatig klonen van iemands stem is strafbaar. Dit wordt gezien als identiteitsfraude. Ook is het een ernstige inbreuk op iemands privacy.

Tips (wat kun jezelf doen)?

- Hang bij een verdacht telefoongesprek direct op.
- Bel de persoon om wie het lijkt te gaan terug op diens eigen nummer
- Stel de persoon vragen over iets waar alleen diegene antwoord op kan geven. Kijk uit dat je niet naar iets vraag wat online over je te vinden is, zoals op social media.
- Spreek een codewoord af: een soort wachtwoord om snel na te kunnen gaan of het daadwerkelijk die persoon is of niet.
- Degene waarmee u praat dringt aan op het investeren, vraagt je om geld of om persoonlijke (bank) gegevens.
- Let op met wat u deelt. Opnames van u kan iemand gebruiken om u na te doen. Vertel of post geen geheime dingen van uzelf online. Dit kunnen criminelen gebruiken om vertrouwen te winnen bij uzelf of iemand die u kent.





Online criminaliteit

Hoe te voorkomen?

Iedereen loopt risico slachtoffer te worden van online criminaliteit. Het is belangrijk om uw risico op slachtofferschap en de gevolgen daarvan klein te houden.

In dit informatieblad leest u hoe u zich eenvoudig kunt beschermen.

Controleer de link voordat u klikt

Criminelen kunnen persoonlijke gegevens

achterhalen,

geld stelen, kwaadaardige software of virussen op apparaten plaatsen als u op een verkeerde link klikt.

- Een veilig webadres (URL) begint met <https://>: en heeft een hangslotje;
- Kijk goed naar de afzender, de aanhef, het taalgebruik men de vormgeving van het bericht;
- Blijf ook oplettend als u de persoon of organisatie kent. Soms ziet het er echt uit maar is het toch nep;
- Vertrouwt u het niet? Neem eerst telefonisch contact op met de persoon, het bedrijf of de organisatie.

Maak nooit zomaar geld over

Let op wanneer u gevraagd wordt geld te overmaken. Een bekende dringend financiële hulp nodig heeft.

Met

een onverwachte en zeer dringende boodschap hopen

criminelen u te overtuigen geld, vertrouwelijke

gegevens of toegang tot apparaten te geven.

Maak alleen verbinding met vertrouwde en beveiligde wifinetwerken

Wanneer u gebruik maakt van openbare of onbeveiligde wifinetwerken, kunnen anderen mogelijk zien wat u op het internet doet en welke gegevens u verstuurt.

- Verstuur geen gevoelige gegevens (e-mail, internetbankieren) over wifinetwerken die u niet kent of niet vertrouwt;
- Zorg dat de wifinetwerken die u (onder andere thuis) gebruikt beveiligd zijn met een gegevensversleuteling;
- Wilt u toch gebruik maken van openbare wifinetwerken? Gebruik dan een versleutelde verbinding (VPN).

Installeer alleen apps via de officiële applicatiewinkel

Criminelen kunnen via apps kwaadaardige software of virussen op uw apparaten plaatsen. Zij kunnen dan meekijken op uw apparaat, bestanden beschadigen of verwijderen en (door middel van chantage) u geld afhandig maken.

- Installeer apps altijd alleen via de officiële applicatiewinkels, zoals de Windows store, de App store en Google Play;
- Controleer tot welke gegevens de app toegang krijgt;
- Bekijk de beoordelingen van medegebruikers om een beeld te vormen van de betrouwbaarheid van de app.

Zorg voor sterke en unieke wachtwoorden

Met zwakke wachtwoorden kan een crimineel aan uw persoonlijke gegevens komen, zoals uw bankgegevens.

- Kies geen veelgebruikte of voor de hand liggende wachtwoorden, zoals uw geboortedatum of telefoonnummer;
- Gebruik een wachtwoord(zin) van minimaal 12 tekens, waaronder speciale tekens als cijfers en leestekens;
- Controleer of uw wachtwoord(zin) sterk genoeg is met de wachtwoordkraaktest op veiliginternetten.nl;
- Het is belangrijk dat u verschillende wachtwoorden gebruikt voor uw apparaten en accounts. In een wachtwoordmanager kunt u de wachtwoorden opslaan;
- Maak gebruik van tweestapsinlog. Naast gebruikersnaam en wachtwoord, moet u dan ook uw identiteit bevestigen met een toegangscode of vingerafdruk.

Doe direct uw updates

Het is belangrijk dat u uw apparaten en apps beveiligd door regelmatig updates uit te voeren. Wanneer u dit niet tijdig doet kan gemakkelijk ingebroken worden op uw apparaten.

- Krijgt u een melding om een update te doen? Stel dit niet uit en doe dit direct;
- Breng in kaart welke apparaten u in huis heeft die verbonden zijn met internet. Ga naar de instellingen van uw apparaten en stel 'automatisch updates' in;
- Mocht het niet mogelijk zijn om het apparaat automatisch te laten updaten, zet dan een herinnering in uw agenda om zelf de updates uit te voeren.

Gebruik een virusscanner

Een virusscanner kan u beschermen tegen veelvoorkomende kwaadaardige programma's.

- Welk antivirusprogramma het beste bij u past, is afhankelijk van uw computeractiviteiten en de manier waarop de virusscanner infecties opspoorst en bestrijdt;
- Let op dat u geen 'nep-antivirus' downloadt, waarmee u uw apparaat infecteert met een virus;
- Laat de antivirusscanner regelmatig uw apparaten scannen.

Maak regelmatig back-ups

Wanneer een crimineel uw apparaat toch heeft kunnen besmetten met een virus of andere kwaadaardige software, dan kunnen zij uw bestanden vernietigen of beschadigen.

- Maak dagelijks een back-up van uw waardevolle bestanden;
- Zorg ervoor dat de back-up losgekoppeld is van uw apparaat.

Toch slachtoffer geworden? Wat nu?

- Melding of aangifte helpt bij het tegengaan van digitale criminaliteit, ook als u geen schade heeft. U kunt aangifte of melding doen bij de politie (0900-8844), Fraudhelpline (088-7867372) en/of Meld Misdaad Anoniem (0800-7000).
- Heeft u behoefte aan meer ondersteuning of advies, neem dan contact op met Slachtofferhulp Nederland (0900-0101).
- Is u geld afhandig gemaakt, heeft u het vermoeden dat iemand uw beveiligingscodes heeft of is uw bankpas kwijt, bel dan direct uw bank via het bij u bekende telefoonnummer.
- Wijzig direct uw gebruikersnamen en beveiligingsinlogcodes. Doe dit vanaf een apparaat dat niet besmet is met schadelijke software

Informatiepunten en aangiften digitale criminaliteit

Aangifte doen bij de politie

Als je (vermoed dat je) slachtoffer bent geworden van digitale criminaliteit, dan kun je aangifte doen bij de politie. Op de website van de politie vind je meer informatie over voor welke vormen van digitale criminaliteit en hoe je aangifte kunt doen: <https://www.politie.nl/aangifte-of-melding-doen/aangifte-van-oplichting.html>.

Informatiepunten Digitale Overheid (IDO's)

IDO's zijn hulppunten waar je je vragen kunt stellen over digitale overheidsdiensten. Deze punten vind je bijvoorbeeld in bibliotheken, of andere locaties in je gemeente. Heb je bijvoorbeeld vragen over je DigiD, dan kun je ze stellen bij een IDO. Op deze website vind je IDO's bij jou in de buurt: <https://www.informatiepuntdigitaleoverheid.nl>.

FraudeHelpdesk

De FraudeHelpdesk is een telefonisch bereikbaar loket dat slachtoffers helpt als ze te maken hebben gehad met digitale oplichting. Ze geven aan welke stappen je kan nemen en hebben veel tips voor het voorkomen van fraude. De website van de FraudeHelpdesk vind je hier: <https://www.fraudehelpdesk.nl/>

Digihulplijn

De Digihulplijn is een telefonisch bereikbaar loket dat mensen helpt met digitale apparaten. Als iemand technische problemen heeft met een apparaat kan diegene bellen met de DigiHulplijn om geholpen te worden. De website van de DigiHulplijn vind je hier: <https://digihulp.nl/>.



Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is een onafhankelijke stichting die partijen en veiligheidsprofessionals helpt om Nederland veiliger en leefbaarder te maken.

Centrum voor Criminaliteitspreventie en Veiligheid
Churchillaan 11, 3527 GV Utrecht
Postbus 14069, 3508 SC Utrecht

T (030) 751 6700
E info@hetccv.nl
I www.hetccv.nl

