CCV centrum voor criminaliteitspreventie en veiligheid

Echt of nep? Cyberweerbaarheid voor senioren

Handleiding interactieve film

Versie 2.0
Oktober 2024

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 en 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 PowerPoint-presentatie 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. Verder omvat ieder filmpje nog twee dia's met informatie over het delicht en tips om oplichting te voorkomen.

Film opvragen

De film is gemaakt door de VeiligheidsAlliantie regio Rotterdam (VAR). Iedereen die de film wil gebruiken kan deze gratis opvragen bij de VAR door te mailen naar var.rotterdam@politie.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:

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

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 en een factsheet met informatiepunten over digitale criminaliteit dat je hiervoor kunt gebruiken. Print deze uit en leg ze op de tafel.

Zorg voor voldoende koffie en 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. Daardoor ben je soms sneller door de presentatie heen dan andere keren.

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

Het programma kun je zelf invullen. Denk bijvoorbeeld aan:

- Inloop (30 minuten)
- Welkom (10 minuten)
- Twee filmpjes: Whatsappfraude en phishing (30 minuten)
- Pauze (20 minuten)
- Drie filmpjes: bankhelpdeskfraude, spoofing en datingfraude (30 minuten).
- Na afloop van de bijeenkomst nog napraten (30 minuten)

Dingen die je nodig hebt

De film wordt afgespeeld via een PowerPoint-bestand. Om de film af te spelen, is een laptop met PowerPoint nodig. 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 dat je laptop een HDMI-aansluiting heeft, of zorg voor een verloopstukje dat in je laptop past en een HDMI-aansluiting bevat.

Verder heb je twee microfoons nodig: 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 een of twee ondersteuners.

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 laat de filmpjes zien, licht deze toe en gaat in gesprek met de deelnemers: Wat zouden zij nu doen? 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. Als er veel mensen komen dan is het handig om meerdere ondersteuners te hebben.

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 iemand uit die deze kennis wel heeft. 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 moet doen tijdens de bijeenkomst en waar hij of zij op moet letten.

Voorbereiding

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 7. In de PowerPoint-presentatie zit een instinker. Wees je hier bewust van.

Print de notities in de bijlage op pagina 16 t/m 20 uit, zodat je deze bij de hand kunt houden tijdens de presentatie. De vetgedrukte tips staan in de PowerPoint-presentatie. De andere tips kun je er bij vertellen.

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, dat er ook criminelen zijn die hier misbruik van maken. In deze bijeenkomst leren de deelnemers hoe zij digitale oplichting kunnen 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 het eerste filmpje en de eerste scène start automatisch. Aan het eind van de scène stopt het filmpje. Je gaat nu in gesprek met de deelnemers. Wat hebben ze gezien?

De presentatie geeft nu een keuzemogelijkheid: reageren of negeren? Je vraagt aan de deelnemers wat zij 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 de gekozen scène waarna deze 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.

Na de film

Na de afloop van de film kun je deelnemers nog de volgende adviezen of tips geven:

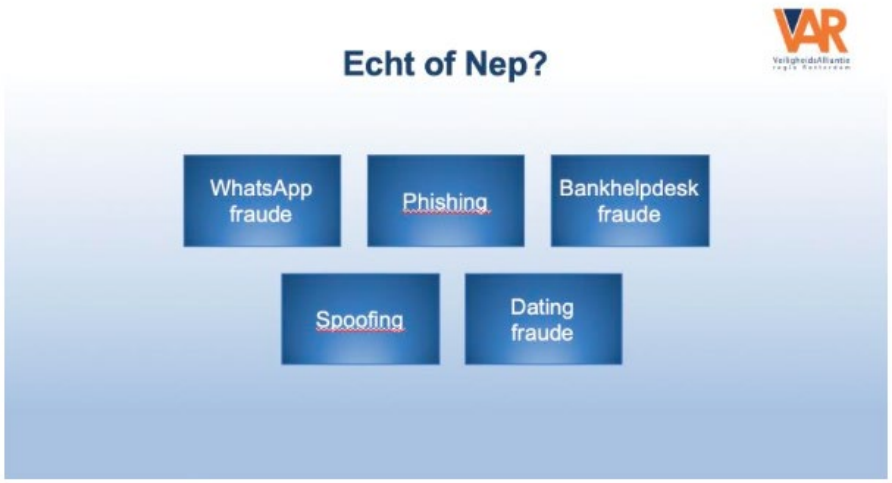
- Het internet is niet eng. Er zijn risico's, maar het zijn geen directe gevaren.
- Je hebt zelf de controle en je kunt kiezen om iets wel of niet te vertrouwen. Ook kun je een mail altijd nog terugvinden in de prullenbak van je mailbox, als je hem hebt verwijderd.
- Klik nooit zomaar op een link die je ontvangt en check altijd dubbel. Wie is de afzender? Klopt het adres? Kreeg je de mail op een vreemd tijdstip zoals midden in de nacht? Staat er in de link geen .nl, maar bijvoorbeeld iets willekeurigs zoals .ndkshfsku? Klik dan niet op de link.
- Vertel de deelnemers dat het niet erg is om een mail te verwijderen, wanneer je het niet vertrouwt. Instanties zoals de Belastingdienst sturen je altijd een vervolgmail. Vaak sturen ze je zelfs een brief op papier, wanneer het om belangrijke informatie gaat. Twijfel je? Dan kun je altijd de instantie bellen om na te vragen of zij je hebben gemaild.
- Benadruk dat mensen zich niet hoeven te schamen als ze slachtoffer zijn geworden. Geef aan dat iemand niet dom is als het hem/haar is overkomen. Criminelen zijn gewoon erg handig en slim. Het kan iedereen overkomen. Maar meld het wel en doe het liefst aangifte.

4 Hoe werkt de film?

Hier lees je stap voor stap hoe het PowerPoint-bestand werkt en hoe je de film kunt afspelen.

Stap 1

Eerst start je PowerPoint op en open je het PowerPoint-bestand ‘Echt of Nep.pptx’. In PowerPoint kies je nu voor ‘afspelen vanaf het begin’. Je krijgt dan een overzicht van de vijf delicten.



Start met het onderwerp linksboven (WhatsApp-fraude). Na het doorlopen van dit deel van de presentatie, kom je automatisch weer terug op het beginscherm. Kies dan voor het volgende delict. Werk van links naar rechts en van boven naar beneden.

Stap 2

Nadat je op de knop ‘WhatsApp-fraude’ hebt geklikt, start automatisch de eerste scène. Ieder delict omvat uit een filmpje dat bestaat uit drie scènes en twee dia’s met informatie en tips. De scènes duren tussen de 30 en 90 seconden. Als de scène is afgespeeld, verschijnt automatisch het eerste keuzescherm.

Overleg met de zaal wat 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 de volgende scène afgespeeld.

Stap 3

Na het afspelen verschijnt er weer een keuzescherm. Met dat keuzescherm 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

Let op: nu volgt een instinker!

Na het bekijken van ‘de andere keuze’ (in dit voorbeeld ‘negeren), kom je automatisch weer terug op een keuzescherm. 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!**

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

Als dit je toch overkomt, sluit dan de PowerPoint-presentatie 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 20) vind je voor ieder delict een bredere uitleg. Deze kun je bij je presentatie gebruiken.

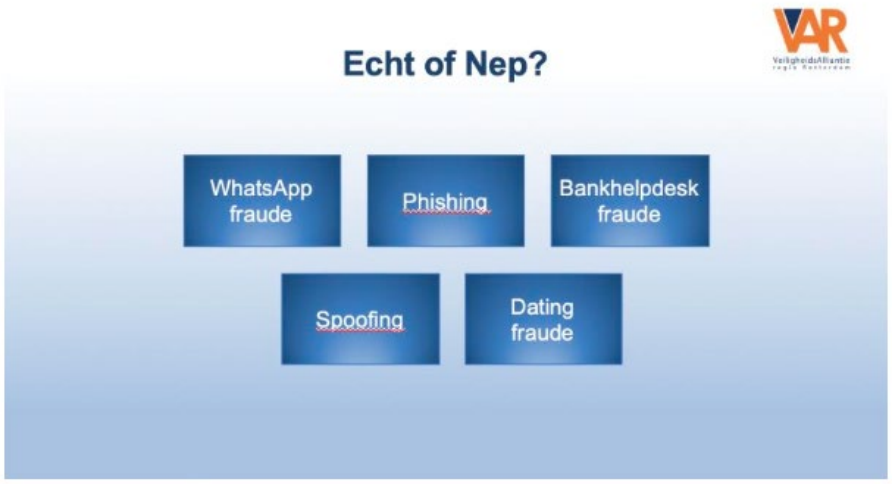
Na de uitleg over het delict, klik je op tips. Je gaat dan naar de volgende dia.

Stap 6

Op de dia staan de drie belangrijkste tips (voorbeeld: zie afbeelding 6). In de notities met bredere uitleg staan deze tips ook. Dat zijn de vetgedrukte zinnen. Daarnaast vind je voor ieder delict nog meer tips. Bespreek de tips met de zaal.

Stap 7

Als het onderwerp is afgesloten, klik je op 'Terug naar start'. Je komt dan weer op het beginscherm met een overzicht van de vijf delicten. Kies dan voor het volgende delict. Werk van links naar rechts en van boven naar beneden.



Alle andere vormen van digitale criminaliteit zijn op dezelfde manier opgebouwd als het voorbeeld van WhatsApp-fraude. Ieder filmpje omvat drie scènes en twee dia's met informatei en tips.

Notities

Extra informatie over de verschillende delicten en de tips staan in de notities bij de dia's. Maar ook in deze handleiding in de bijlagen (pagina 16 t/m 20). Gebruik deze notities tijdens de presentatie als extra ondersteuning. De vetgedrukt tips staan vermeld op de dia's. De andere tips zijn aanvullend.

5 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.

Bijlagen met hulpmiddelen

Voorbeeldtekst uitnodiging bijeenkomst film Echt of Nep?

Echt of Nep? Een bijeenkomst voor 65-plussers 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 en geld van u te stelen.

Daarom organiseert XXX op XXX de bijeenkomst *Echt of Nep*? Deze bijeenkomst is voor 65-plussers 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 met film Echt of Nep?

Wat moet je regelen voor een bijeenkomst Echt of Nep?

- ☐ PowerPoint-bestand met de film
- ☐ 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 daarop het PowerPoint-bestand en 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 WhatsApp fraude bij film Echt of Nep?

Wat is 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 met wat iemand zelf kan doen (vetgedrukte tips staan op dia).

- **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 persoon 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 bij film Echt of Nep?

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 met wat iemand zelf kan doen (vetgedrukte tips staan op dia).

- **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 bij film Echt of Nep?

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 met wat iemand zelf kan doen (vetgedrukte tips staan op dia).

- **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 bij film Echt of Nep?

Wat is Spoofing?

Tekst in beeld
Bij spoofing gebruiken internetcriminelen een identiteit, e-mailadres 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 met wat iemand zelf kan doen (vetgedrukte tips staan op dia).

- **Gaat het om geld en is er haast bij? Vertrouw dit niet. Eerst checken dan klikken.**
- **Klik nooit op een link die je 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 je 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 bij film Echt of Nep?

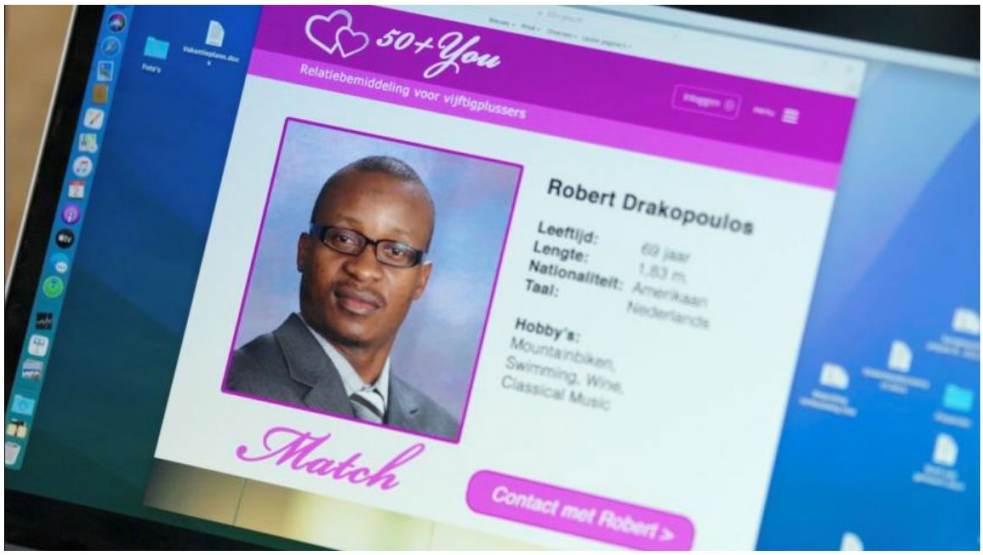
Wat is datingfraude?

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 je. Hij of zij zorg ervoor dat je hem of haar gaat vertrouwen 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 met wat iemand zelf kan doen (vetgedrukte tips staan op dia).

- **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 je te isoleren om je zo 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/



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 ongevraagd helpdeskadvies krijgt of een bekende dringend financiële hulp nodig heeft. Met
een onverwachtse en zeer dringende boodschap hopen
criminelen u te overtuigen geld, vertrouwelijke gegevens of toegang tot apparaten te geven.

- Criminelen kunnen misbruik maken van een bekend telefoonnummer. Enkel het telefoonnummer controleren is daarom niet voldoende;
- Verbreek het contact en (video)bel ter controle het nummer van de persoon, het bedrijf of de organisatie die bij u bekend is;
- Maak geen geld over, deel geen persoonlijke gegevens en geef nooit iemand zomaar toegang tot uw apparaten;
- Houd uw pincodes en inlog- of beveiligingscodes altijd geheim en sta nooit uw bankpas, creditcard of inlogapparaatje af;

Bedenk goed wat u met wie deelt op het internet

Criminelen kunnen uw persoonlijke gegevens gebruiken om u of mensen uit uw omgeving op te lichten.

- Blijf bewust van wat u deelt. Zo makkelijk als het is om iets op internet te plaatsen, zo moeilijk is het om dit er weer af te krijgen;
- Laat u uw gegevens ergens achter, ga na wie toegang krijgt tot deze gegevens en hoe lang deze gegevens te zien zijn;
- Geef niet meer gegevens dan noodzakelijk.

Versie 2023
VeiligheidsAlliantie regio Rotterdam

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 wifi-netwerken? 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 beveiligt 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 updaten' 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 opspoort 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 vergrendelen 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), Fraudehelpdesk (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 beveiligings- en inlogcodes. Doe dit vanaf een apparaat dat niet besmet is met schadelijke software

Informatiepunten en aangifte digitale criminaliteit

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 wil zoveel mogelijk voorkomen dat iemand slachtoffer wordt van fraude zoals digitale oplichting. De Fraudehelpdesk geeft allerlei praktische tips om oplichting tegen te gaan. Ook helpt de Fraudehelpdesk slachtoffers door advies te geven en iemand naar de juiste instantie te verwijzen. De website vind je hier: https://www.fraudehelpdesk.nl/

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 vormen van digitale criminaliteit en hoe je aangifte kunt doen: https://www.politie.nl/aangifte-of-melding-doen/aangifte-van-oplichting.html.

Digital trust centre (ministerie van Economische Zaken en Klimaat)

Op het platform 'digital trust centre' van het ministerie van Economische Zaken en Klimaat vind je meer informatie over het doen van aangifte bij digitale criminaliteit. Ook vind je hier verschillende aangifteformulieren. De website van de het 'digital trust centre' vind je hier: https://www.digitaltrustcenter.nl/informatie-advies/aangifte-of-melding-doen.

CCV centrum voor criminaliteitspreventie en veiligheid

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
Churchilllaan 11, 3527 GV Utrecht
Postbus 14069, 3508 SC Utrecht

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