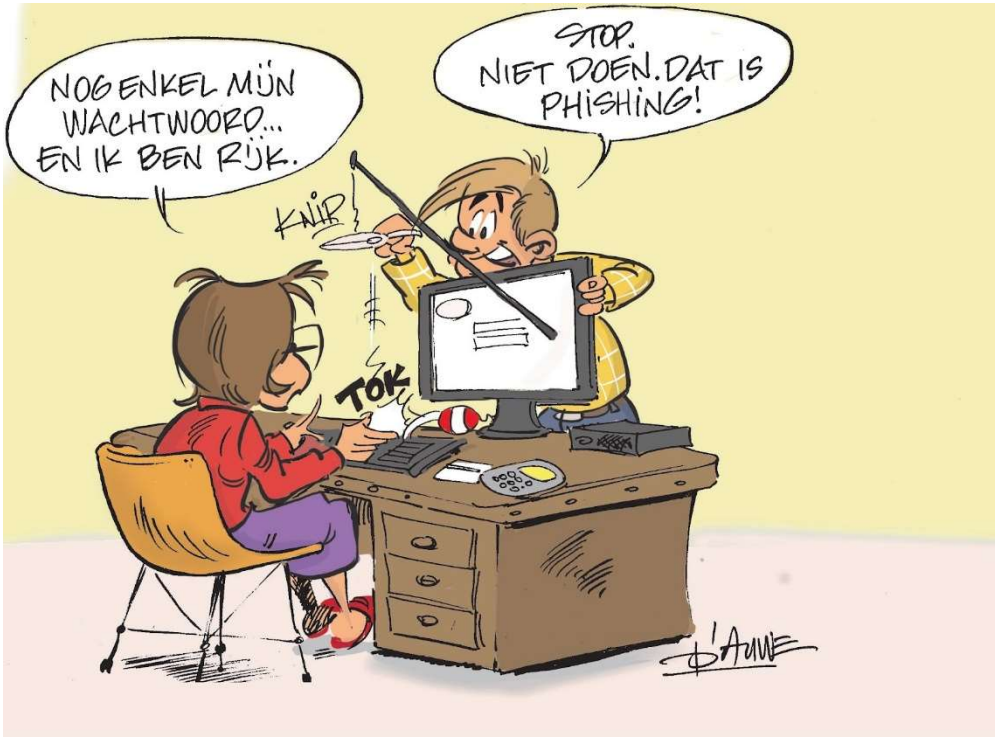
# CYBERPREVENTIEADVISEUR
# DRAAIBOEK VOOR LOKALE BESTUREN & POLITIEZONES




Gouverneur
Provincie Antwerpen
Cathy Berx

BIN Kenniscentrum
Buurt.Informatie.Netwerk

provincie gouverneur
Vlaams-Brabant
Jan Spooren

KORTRIJK

POLITIE ANTWERPEN

# Inhoudsopgave

# 1. Inleiding

We kunnen ons een wereld zonder internet niet meer voorstellen. We shoppen en bankieren online, delen persoonlijke informatie via sociale media en zijn altijd en overal bereikbaar.
Ook criminelen merken dit op en gaan steeds vaker 'online' te werk. Cybercriminaliteit vormt een steeds groter wordend deel van de criminaliteitsstatistieken.
De digitalisering van de samenleving zorgt voor een veranderend veiligheidslandschap en vraagt om een vernieuwende, creatieve aanpak.

Het BIN Kenniscentrum, de stad Kortrijk, de federale diensten van de gouverneurs van Antwerpen en Vlaams-Brabant en de lokale politie van de zone Antwerpen slaan de handen in elkaar om het project 'cyberpreventieadviseurs' vorm te geven.

*"De strijd tegen cybercrime is nodig en tegelijk erg complex. Om hem te winnen, of minstens niet compleet te verliezen, moeten we hem samen voeren. Ieder van ons kan slachtoffer worden. We willen dan ook het bewustzijn over cyberveiligheid versterken, tips en bruikbare informatie aanreiken om iedereen, jong en oud, beter te wapenen tegen de vele digitale gevaren." Cathy Berx, gouverneur provincie Antwerpen*

De organiserende overheden willen hun inwoners weerbaarder maken tegen cybercriminaliteit en dit aan de hand van 10 concrete tips. Deze eenvoudige, maar doeltreffende tips maken het project laagdrempelig en toegankelijk voor iedereen die wel eens op het internet surft.

In een eerste fase namen een handvol pilootregio's deel aan het project zodat we snel maar daadkrachtig van start konden gaan.

Vandaag is het project 'cyberpreventieadviseur' klaar om verder uitgerold te worden naar andere politiezones, steden en gemeenten in de provincie Antwerpen.
Met dit draaiboek willen we de lokale besturen en politiezones een beeld geven over het project 'cyberpreventieadviseur' en praktische informatie aanbieden voor een vlotte opstart.

Speciale dank aan de pilootregio's:
Vlaams-Brabant: politiezones Zennevallei, Pajottenland, Kastze, Lubbeek en stad Diest
Antwerpen: gemeente Kapellen, gemeente en politiezone Brasschaat
Stad Kortrijk

# 2. Het project ‘cyberpreventieadviseur’

## 2.1 Doel

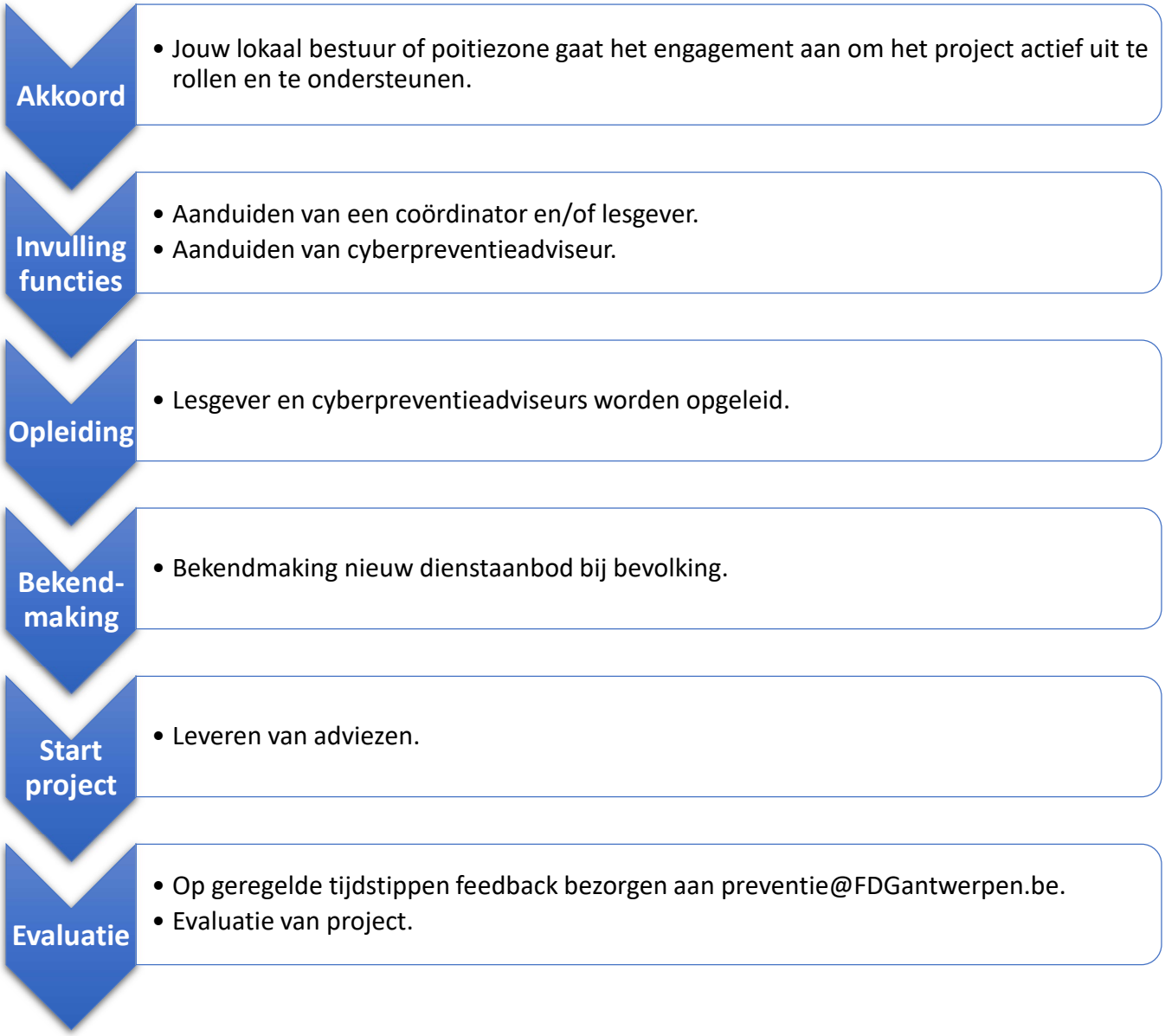
Het project ‘cyberpreventieadviseur’ of ‘CPA’ zet volop in op de zelfredzaamheid van de burger en het verwerven van digitale inzichten en vaardigheden. De CPA gaat aan de slag met tien concrete tips en tracht zo zijn luisteraar weerbaarder te maken tegen cybercrime. De tips zijn zo opgesteld dat iedereen er dadelijk mee aan de slag kan.
Het project wil iedere surfende burger enkele goede reflexen aanleren en onbezonnen gewoonten ontraden zoals bv. info met iedereen delen, of je bankzaken verrichten via een openbaar WIFI-netwerk.

De focus ligt op het voorkomen van de meest gebruikelijke fenomenen inzake cybercrime zoals phishing, online aan- en verkoopfraude en vriendschapsfraude.

De cyberpreventieadviseur biedt echter geen ondersteuning bij technische problemen of helpt je niet met het configureren van jouw smartphone of PC.
Bij meer complexe of specifieke problemen verwijst de CPA door naar de gepaste helpdesk.

## 2.2 In 6 stappen tot cyberpreventieadviseur

Om in te stappen in het project cyberpreventieadviseur, doorloop je als lokaal bestuur of politiezone zes stappen.
Elk van deze stappen krijgt hieronder een korte verduidelijking met bijhorende timing.




### 2.2.1 Akkoord van alle betrokken partners

Uiteraard is het belangrijk dat alle betrokken partners en diensten het project dragen en ondersteunen.

Voordat een lokaal bestuur of politiezone in het project 'CPA' instapt, is het nodig om enkele knopen door te hakken:

*Hoeveel adviseurs werven we aan ?*

Het is nuttig om op voorhand te bepalen met hoeveel cyberpreventieadviseurs je wil starten. Dit aantal is voor elke gemeente, stad of politiezone verschillend. Het hangt onder meer af van de beschikbare tijd van de coördinator, de bestaande vraag naar ondersteuning en het aantal verwachte adviesaanvragen. Bij het inschakelen van te veel adviseurs is de kans groot dat ze niet goed opgevolgd en begeleid kunnen worden. Bij onvoldoende adviesaanvragen is het moeilijk om de adviseurs actief en gemotiveerd te houden. De opvolging van de werklast is heel belangrijk.

*Schakel je eigen, intern personeel in als adviseur of werk je met vrijwilligers ?*

Als lokaal bestuur heb je uiteraard de vrijheid om de taak als CPA in te vullen zoals het de organisatie het best past. Je hebt hierbij de keuze om eigen personeel op te leiden (vanuit de preventiedienst of lokale politiezone), dan wel om vrijwilligers aan te werven om het team te versterken.

Kandidaat-vrijwilligers kunnen gerekruteerd worden via een oproep in de lokale media, bv. via het infoblad of de website van de gemeente, via de website van de politie, via de communicatiekanalen van de buurtinformatienetwerken.

In bijlage lees je een voorbeeld van aanwervingstekst, een afsprakennota en legitimatiekaart.

- ➔ *Wil je meer te weten komen over het werken met vrijwilligers? Wij kunnen je het draaiboek 'Vrijwilligers helpen inbraken voorkomen' van de Federale diensten Vlaams-Brabant bezorgen. Je kan het opvragen via preventie@FDGantwerpen.be.*
- ➔ *De meest actuele richtlijnen en wetgeving omtrent vrijwilligerswerk zoals verzekering en onkostenvergoeding, kan je via https://www.vlaanderenvrijwilligt.be/ raadplegen.*
- ➔ *TIP: Je kan gericht op zoek gaan naar geschikte vrijwilligers. Ken je een politieman op rust die nog steeds geëngageerd is? Ken je een helpdeskmedewerker die openstaat voor vrijwilligerswerk? Spreek hen actief aan en leg het project kort uit. Wie weet ontstaat er een mooie samenwerking.*

  *Nadien worden de kandidaat-vrijwilligers uitgebreid geïnformeerd over de taken, de doelstellingen, de selectie, de ondersteuning, de opleiding… Zo weten ze waar ze zich mogen aan verwachten en kunnen ze beslissen om zich al dan niet kandidaat te stellen.*

Is de knoop doorgehakt en wil je graag instappen in het project 'cyberpreventieadviseur'? Breng ons op de hoogte via preventie@FDGantwerpen.be en we bezorgen je alle concrete informatie.

### 2.2.2 Invullen van de functies

#### Cyberpreventieadviseur

Het is belangrijk te onderstrepen dat de cyberpreventieadviseur geen specifieke voorkennis over het thema moet hebben. Hij volgt een basisopleiding waarbij hij handvaten krijgt aangereikt om burgers grondig te informeren over het onderwerp.
De adviseur kan gebruik maken van presentaties, flyers, materiaal, … om het advies te verduidelijken. Dit materiaal kan verkregen worden via het Bin Kenniscentrum (info@bin-plp.be).

Een duidelijk takenpakket en profiel van de CPA moet voor ogen gehouden worden. Deze functieomschrijving vormt de basis om de juiste personen aan te stellen of aan te werven. Het document verduidelijkt onder meer dat de adviseur een basisopleiding volgt en beschikt over de nodige communicatieve en sociale vaardigheden. Een uitgebreid functieprofiel wordt in bijlage toegevoegd.

De hoofdtaken van een cyberpreventieadviseur bestaan uit activeren, adviseren en doorverwijzen.

*Activeren*

De CPA brengt burgers op de hoogte van activiteiten rond cyberpreventie door bijv. flyers rond te brengen of berichten door te sturen.

*Adviseren*

- 1-op-1-advies
  Tijdens een individueel advies, gaat de cyberpreventieadviseur bij de aanvrager langs om een korte toelichting te geven. Hierbij kan dieper ingegaan worden op de specifieke vragen van de burger.
- Infosessies
  Tijdens bijeenkomsten geven de adviseurs een toelichting over digitale veiligheid en beantwoorden ze vragen.

*Tip: Toets op voorhand naar de verwachtingen van zowel de adviseur als de aanvrager om zo de meest gepaste combinatie te bekomen. De ene adviseur geeft bijvoorbeeld liever persoonlijk advies terwijl een andere adviseur graag voor* groepen spreekt.

*Doorverwijzen*

Niet iedere vraag kan altijd direct worden opgelost door de CPA. Daarom is de adviseur goed op de hoogte van de partners waarnaar doorverwezen kan worden. Als ze de juiste partner niet kennen, noteren ze de vraag en bezorgen ze later het antwoord aan de burger.

Tijdens het uitvoeren van zijn taken houdt de cyberpreventieadviseur zich aan vooraf bepaalde spelregels. De (spel)regels dienen om het handelingskader van de CPA af te bakenen en om aan te geven waar hij wél en niet voor ingezet kan worden. De spelregels zijn dynamisch en in ontwikkeling.

| | |
|---|---|
| HANDS-OFF | •De CPA geeft enkel mondeling advies, geen directe ondersteuning op computer, tablet of smartphone.<br>•De CPA geeft geen mondelinge begeleiding doorheen het proces. |
| DOORVERWIJZEN | •De CPA is opgeleid tot een basisniveau. Voor diepgaandere vragen of meldingen verwijzen ze door naar de juiste (veiligheids)partner |
| DYNAMISCH | •De rol van de CPA kan veranderen. De wensen en behoeften van de adviseurs en bewoners zijn hierbij leidend.<br>•De CPA houdt zich aan de opgestelde regels. |
| PRIVACY | •De CPA krijgt nooit toegang tot gevoelige (persoons)gegevens. |

De cyberpreventieadviseur benadrukt tijdens elk advies of elke infoavond dat het naleven van de preventietips het risico op cybercriminaliteit verkleint. Hij, noch de organisatie, gemeente of politiezone achter deze campagne, kan aansprakelijk worden gesteld indien een burger toch slachtoffer zou worden van enige vorm van cybercriminaliteit.

## Coördinator

Een coördinator die voldoende tijd, ruimte en materiaal krijgt, is een essentiële voorwaarde voor het welslagen van het project. De coördinator is verbonden aan de gemeentelijke preventiedienst of politiedienst. Deze coördinator heeft (bij voorkeur) de basisopleiding tot cyberpreventieadviseur zelf gevolgd.

Een coördinator zet krijtlijnen uit, maakt reclame voor cyberpreventieadvies, ondersteunt, motiveert, informeert, evalueert en stuurt de (vrijwillige) CPA aan bij het verlenen van adviezen. Hij blijft op de hoogte van de actuele ontwikkelingen in het cyberpreventielandschap. De coördinator is het aanspreekpunt voor de burger, de CPA, het Bin Kenniscentrum en de federale diensten van de gouverneur.

De coördinator bezorgt de adviseurs correcte informatie over de aanvragen, belegt regelmatig vergaderingen en zorgt voor de nodige ondersteuning inzake informatie en materiaal.

### *Verzamelen en beheren van aanvragen*

De coördinator beheert de ontvangen aanvragen en wijst ze toe aan de CPA. Dit kan op volgende manieren:

- *<u>De coördinator stuurt de contactgegevens van de aanvrager via mail door:</u> de CPA neemt zelf contact op met de aanvrager. Dit houdt een minimale werklast in voor de coördinator. De adviseur bepaalt zelf wanneer de afspraak doorgaat. Het vergt meer inspanningen van de adviseur maar hij krijgt meer vrijheid.*
- *<u>De coördinator legt zelf de afspraak vast:</u> de coördinator vraagt bijvoorbeeld telkens de vrije momenten gedurende de twee volgende weken van de adviseurs op. Dit vergt meer inspanningen van de coördinator. Deze werkwijze kan meer vertrouwen geven aan de aanvrager omdat de politie/gemeente de afspraak vastlegt en meedeelt wie het bezoek zal uitvoeren. De CPA is enkel verantwoordelijk voor het uitvoeren van het advies en het opstellen van het verslag.*

### *Organiseren van overlegmomenten*

Uit ervaring blijkt dat zowel coördinatoren als de adviseurs periodieke overlegmomenten zinvol vinden. Tijdens dergelijke samenkomsten leren de adviseurs de coördinator en elkaar

kennen. Verder wisselen ze ervaringen en informatie uit en bespreken ze moeilijke huisbezoeken. De coördinator bewaakt het verloop van deze vergaderingen en luistert naar de voorstellen van de adviseurs.

#### Lesgever

Naast de coördinator moet er ook een lesgever aangeduid worden die de materie aan de adviseurs overbrengt. Een coördinator kan deze taak op zich nemen, maar dit is niet noodzakelijk.
De concrete invulling van het takenpakket van de lesgever, lees je onder het volgend punt 'opleiding'.

### 2.2.3 Opleiding

De federale diensten van de gouverneur bieden samen met hun partners een eerste basisopleiding aan gebaseerd op het 'teach-the-theacher' principe. De opleiding duurt 8 uur en wordt verspreid over twee halve opleidingsdagen.

De lokale besturen duiden een lesgever aan die op zijn beurt de materie overbrengt naar de adviseurs. Het is mogelijk dat de besturen samenwerken en één lesgever aanduiden voor meerdere regio's.
De opleiding voor de cyberpreventieadviseurs wordt lokaal georganiseerd. De lesgevers ontvangen de nodige documenten ter ondersteuning via het Bin Kenniscentrum.

De opleiding focust zich zowel op de meest voorkomende cybermisdrijven als op de tips die deze misdrijven helpen voorkomen.
Het blijft een basisopleiding ter preventie van cybercriminaliteit. De cyberpreventieadviseur is geen helpdeskmedewerker of IT-specialist. Indien een burger andere hulp of ondersteuning nodig heeft, wordt hij doorverwezen naar meer geschikte organisaties.

### 2.2.4 Oproep voor adviezen

Nu de cyberpreventieadviseurs zijn opgeleid en de taakverdeling op punt staat, is het tijd om inwoners warm te maken voor het nieuwe dienstaanbod.

Dit kan via een oproep in de lokale media of via de lokale communicatiemiddelen zoals een infoblad of website.
Vergeet zeker bestaande verenigingen (bv. BIN, KWB, seniorenraad, …) niet op de hoogte te brengen van het project. Vaak zijn zij geïnteresseerd in veiligheidsthema's en willen ze graag samen een infoavond organiseren.

In bijlage vind je een inspiratietekst om adviezen te verzamelen.

### 2.2.5 Start van het project

Zodra je de eerste aanvragen ontvangt, kan de adviseur van start. Uit een eerste pilootfase blijkt dat het nuttig is om de CPA'ers in duo te laten starten. Een eerste infosessie voor het eigen personeel is een win-win. De CPA doet vertrouwen op en kan zijn presentatie uittesten. Daarnaast is het eigen personeel op de hoogte van het nieuwe project en kan de CPA de gegeven tips meenemen.

### 2.2.6 Evaluatie en bijsturing

Cybercriminaliteit is een criminaliteitsvorm die continu evolueert. We moeten dus kritisch blijven over de tips die burgers ontvangen en de manier waarop de adviezen gegeven worden.

De coördinator kan regelmatig feedback vragen aan de aanvragers over de inhoud en de kwaliteit van een advies. Een voorbeelddocument lees je in bijlage.

Door regelmatig feedbackmomenten te organiseren, zowel lokaal als bovenlokaal, willen we tegemoet komen aan dit aandachtspunt.

## 2.3 Aangeboden ondersteuning

### 2.3.1 Opleiding en bijscholing

Om het project 'cyberpreventieadviseur' te doen slagen, is het belangrijk dat elk lokaal bestuur start met dezelfde informatie en inzichten. Daarom worden er periodiek opleidingen voor de lesgevers georganiseerd. Deze opleidingen verlopen in alle deelnemende provincies op een gelijke manier op basis van 10 tips. Lokale zones zijn daarna vrij om eigen accenten toe te voegen.

Aangezien cybercriminaliteit een fenomeen betreft dat continu is evolutie is, zal het BIN Kenniscentrum zorgen voor voortdurende updates via hun communicatiekanalen.

### 2.3.2 Voortdurende ondersteuning

Bij vragen of problemen kan je steeds terecht bij de federale diensten van de gouverneur van Antwerpen (preventie@FDGantwerpen.be) of bij het Bin Kenniscentrum (info@bin-plp.be).

We zorgen dat we up-to-date blijven, ontwikkelen samen met de partners nieuwe initiatieven, flyers, gadgets … maar brengen ook coördinatoren samen om van elkaar te leren en elkaar te ondersteunen.

# BIJLAGEN

## Bijlage 1: Aanwervingstekst vrijwillige cyberpreventieadviseurs

**Gezocht: vrijwillige cyberpreventieadviseurs**

Veiligheid op het internet wordt steeds belangrijker, voor gebruikers van alle leeftijden. Wil jij jouw buur helpen informeren over een betere beveiliging op het internet?

De POLITIEDIENST / PREVENTIEDIENST van (GEMEENTE) zoekt enthousiaste vrijwilligers om hun inwoners te informeren over phishing, privacy en andere digitale valkuilen. Als vrijwillige cyberpreventieadviseur volg je eerst een opleiding die bestaat uit een infosessie gespreid over twee momenten. Na de opleiding ben je klaar om advies te geven aan jouw buren over hoe ze zichzelf het beste beveiligen tegen mogelijk slachtofferschap van cybercriminaliteit.

Geïnteresseerd in cyberveiligheid en cyberpreventie?
Ben je bereid om je als vrijwilliger in te zetten om de cyberweerbaarheid in (GEMEENTE) te verhogen?
Ben je een sociaalvaardig persoon die met veel enthousiasme kennis kan overbrengen?
Deins je niet terug om je kennis over te brengen aan een groep geïnteresseerde buren?

JA? Dan ben jij de persoon die wij zoeken!
Voor meer informatie kan je contact opnemen met: (CONTACTGEGEVENS COORDINATOR CYBERPREVENTIE)

## Bijlage 2: Oproep naar vrijwillige cyberpreventieadviseurs vanuit de BIN-werking

Beste BIN-lid,

Je hebt ongetwijfeld de volgende termen al gehoord of gelezen:

-Phishing – Smishing – Vishing
-Vriendschapsfraude – Whatsapp-fraude
-Geldezels (Money Mules)
-Helpdesk fraude
-Aan- en verkoopfraude via internet
-…

Weet je ook wat deze termen betekenen? En nog belangrijker, weet je wat je kan doen om online fraude te voorkomen?

Jouw BIN stapt mee in een project waarbij we burgers beter willen beschermen tegen cybercriminaliteit.
Het is de bedoeling om de burger via een tiental tips te wapenen tegen de meest voorkomende vormen van online fraude. Om dit op een begrijpelijke en vooral laagdrempelige manier te bereiken doen we een beroep op vrijwilligers.
Wie is er beter geschikt om zich als vrijwilliger aan te bieden dan een BIN-lid dat reeds interesse toont voor de veiligheidsproblematiek?
Als vrijwillige adviseur krijg je natuurlijk de nodige ondersteuning vanuit de politiezone/gemeente en het BIN Kenniscentrum. Enige voorafgaande kennis is geen vereiste. Er wordt gezorgd voor een opleiding op maat van de “leken” onder ons.

Indien je interesse hebt om mee te werken aan dit project en/of je wenst bijkomende informatie kan je contact opnemen met : (gegevens contactpersoon politiezone/gemeente)
Of met Benno Gekiere en Jean Roef van de V.Z.W. BIN Kenniscentrum (benno.gekiere@bin-plp.be, jean.roef@bin-plp.be )

Bijlage 3: Afsprakennota voor de vrijwillige cyberpreventieadviseur

# Afsprakennota – vrijwillige cyberpreventieadviseur

*Deze afsprakennota legt de wederzijdse rechten en plichten van de organisatie en de vrijwilliger vast. Het document omschrijft gemaakte afspraken en biedt een leidraad om ethisch te handelen tijdens het uitvoeren van de opdracht.*

## Rechten en plichten van de organisatie en de vrijwilliger

### 1. Organisatie

| | |
|---|---|
| Naam | Organisatie |
| Adres | xxx |
| Tel.nr | xxx |
| e-mail | xxx |
| Sociale doelstelling | Cybercriminaliteit vormt een steeds groter wordend deel van de criminaliteitsstatistieken. De laatste vijf jaar registeren we maar liefst een verdubbeling van het aantal inbreuken inzake informaticacriminaliteit (bron: statistieken federale politie).<br><br>Ook organisatie merkt een stijging in het aantal meldingen rond cybercriminaliteit en gaat mee de strijd aan tegen dit fenomeen.<br><br>Door o.a. de inzet van cyberpreventieadviseurs willen we:<br>- de weerbaarheid van onze inwoners m.b.t. cybercriminaliteit op een laagdrempelige manier vergroten;<br>- inzetten op zelfredzaamheid en het verwerven van digitale inzichten en vaardigheden;<br>- specifieke doelgroepen zoals slachtoffers, jongeren en senioren extra ondersteuning bieden. |
| Juridisch statuut | Lokale politie / gemeentebestuur |

Verantwoordelijke of gemandateerde voor ondertekening van de afsprakennota.

| | |
|---|---|
| Naam | xxx |
| Functie | Korpschef - burgemeester |

Verantwoordelijke voor informatie over 'rechten en plichten van organisatie en vrijwilliger'.

| | |
|---|---|
| Naam | xxx |
| Functie | xxx |

Verantwoordelijke van de organisatie, die moet verwittigd worden bij ongevallen.

| | |
|---|---|
| Naam | xxx |
| Functie | xxx |
| Tel. - GSM | xxx |

## 2. Aard van het Vrijwilligerswerk

De vrijwilliger vervult de functie van vrijwillige cyberpreventieadviseur (verder de vrijwilliger genoemd).

De vrijwilliger engageert zich om voor de lokale politie - gemeente belangeloos activiteiten te verrichten.

Het takenpakket van de vrijwilliger wordt opgedeeld in twee deeltaken:

- Activeren

  De vrijwilliger ondersteunt de organisatie op lokale informatiemomenten betreffende cyberpreventie.

- Adviseren

  Onder coördinatie van de organisatie gaat de vrijwilliger op (huis)bezoek en geeft hij toelichting over digitale veiligheid en beantwoordt hij gestelde vragen. Dit advies gebeurt op basis van volgende spelregels:

  - Hands-off

    De vrijwilliger geeft enkel mondeling advies, geen directe computerondersteuning.

  - Doorverwijzen

    De vrijwilliger is opgeleid tot een basisniveau. Voor diepgaandere vragen of meldingen verwijst hij door naar de juiste (veiligheids)partners.

  - Dynamisch

    De rol van de vrijwilliger kan wijzigen naargelang de behoefte van de vrijwilliger en organisatie.

  - Privacy

De vrijwilliger krijgt nooit toegang tot gevoelige (persoons)gegevens.

De vrijwilliger:

- volgt hiervoor de basisopleiding "adviseur cyberpreventie";
- neemt zoveel mogelijk deel aan bijscholingen;
- neemt de nodige initiatieven om zijn eigen kennis en vaardigheden inzake digitale veiligheid op peil te houden.

## 3. Verzekeringen

### *3.1. Verplichte verzekering*

| | |
|---|---|
| Waarborgen | De burgerlijke aansprakelijkheid, met uitzondering van de contractuele aansprakelijkheid, van de organisatie en de vrijwilliger. |
| Maatschappij | xxx |
| Polisnummer | xxx |

### *3.2. Vrije verzekeringen*

| | |
|---|---|
| Waarborgen | Lichamelijke schade die geleden is door vrijwilligers bij ongevallen tijdens de uitvoering van het vrijwilligerswerk of op weg naar- en van de activiteiten |
| Maatschappij | xxx |
| Polisnummer | xxx |

| | |
|---|---|
| Waarborgen | Rechtsbijstand voor de twee genoemde risico's |
| Maatschappij | xxx |
| Polisnummer | xxx |

## 4. Vergoedingen

De organisatie betaalt een forfaitaire vergoeding van xx euro (rekening houdend met de wettelijk vastgestelde maxima) voor de onkosten die verbonden zijn aan een advies of bijscholing. Deze onkosten houden onder meer in:

- de verplaatsingskosten om naar de woning of vergaderzaal van de adviesaanvrager te gaan (brandstof, onderhoud en verzekering voertuig);

- de verplaatsingskosten naar de bijscholing (brandstof, onderhoud en verzekering voertuig);
- de kosten van telefonie (en eventueel mail) om de communicatie met de organisatie te voeren;
- …

## 5. Aansprakelijkheid

De organisatie is aansprakelijk voor de schade die de vrijwilliger aan derden veroorzaakt bij het verrichten van vrijwilligerswerk.

Ingeval de vrijwilliger bij het verrichten van het vrijwilligerswerk de organisatie of derden schade berokkent, is hij enkel aansprakelijk voor zijn bedrog en zijn zware schuld.
Voor lichte schuld is hij enkel aansprakelijk als die bij hem eerder gewoonlijk dan toevallig voorkomt.

## 6. Grondhouding en geheimhoudingsplicht

De vrijwilliger benadert iedereen vanuit een respectvolle houding en vermijdt bij zijn werkzaamheden elke vorm van discriminatie.

De vrijwilliger aanvaardt een opdracht enkel indien hij die opdracht binnen een redelijke termijn kan volbrengen en er de nodige aandacht en tijd aan kan besteden.

De vrijwilliger kan op geen enkele wijze vergoed worden door de aanvrager.

De vrijwilliger is in zijn opdracht volledig transparant over de spelregels van zijn opdracht evenals de mogelijkheden en beperkingen die deze inhoudt.

Vanwege de aard van de functie cyberpreventieadviseur, is de vrijwilliger onderworpen aan de geheimhoudingsplicht zoals omschreven in artikel 458 van het Strafwetboek. Hij heeft als fundamentele taak te waken over de vertrouwelijkheid van de informatie.

> *"Geneesheren, heelkundigen, officieren van gezondheid, apothekers, vroedvrouwen en alle andere personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd en deze bekendmaken buiten het geval dat zij geroepen worden om in rechte (of voor een parlementaire onderzoekscommissie) getuigenis af te leggen en buiten het geval dat de wet hen verplicht die geheimen bekend te maken, worden gestraft met gevangenisstraf van acht dagen tot zes maanden en met een geldboete van honderd tot vijfhonderd frank".*

Aangezien de vrijwilliger taken uitvoert in een breder veiligheidslandschap, gaat hij akkoord met een korte screening van zijn profiel onder andere op basis van een uittreksel van het strafregister.

## 7. Wederzijdse rechten en plichten

**De vrijwilliger** heeft recht op informatie over zijn activiteiten, afbakening van zijn werkveld en werktijden, een contactpunt bij conflictsituaties, over aangepaste vorming en bijscholing, …

**De organisatie** heeft recht op een correcte deontologische houding van de vrijwilliger met betrekking tot het naleven van de onderlinge afspraken, het respecteren van de afbakening van het activiteitsveld, …

Dit betekent dat:

- de vrijwilliger werkt onder de coördinatie van de xxx. De vrijwilliger levert geen cyberpreventie-adviezen op eigen initiatief;

- de vrijwilliger respecteert de vastgelegde werkafspraken;
- de vrijwilliger verricht activiteiten voor de organisatie. De vrijwilliger neemt een loyale houding aan die in overeenstemming is met de organisatie waarvoor hij zijn activiteiten verricht;
- de vrijwilliger bewaart steeds een neutrale houding ten overstaan van commerciële initiatieven van cyberbeveiliging;
- de vrijwilliger ontvangt van de organisatie de nodige opleidingen, navormingen en ondersteuning die hem in staat stelt zijn opdracht naar goed behoren uit te oefenen;
- de vrijwilliger wordt steeds tijdig verwittigd van een uit te voeren adviesaanvraag;
- de vrijwilliger informeert steeds tijdig de organisatie over zijn onbeschikbaarheid.

## 8. Naleving van deze afsprakennota

De coördinator ziet erop toe dat de vrijwilliger kennis krijgt van de inhoud van de code en laat hem de tekst ondertekenen.

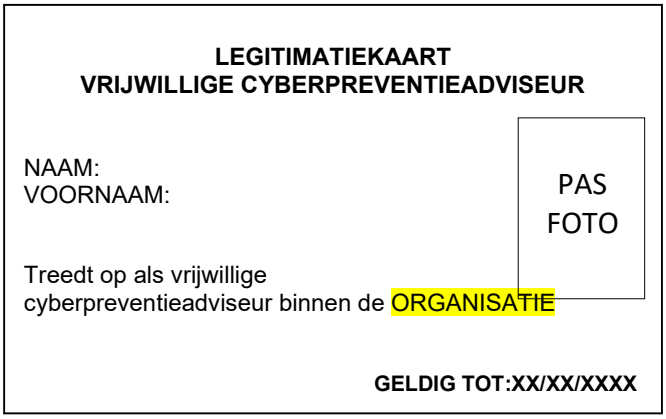
Iedereen die deze afsprakennota in het kader van zijn functie als cyberpreventieadviseur ondertekent, verbindt zich ertoe deze na te leven.

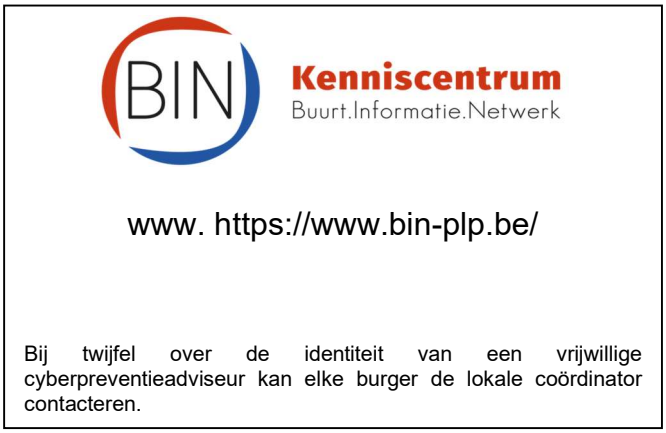
Datum:

Namens het politiecollege / college van burgemeester en schepenen:

De korpschef / secretaris de burgemeester-voorzitter

## Bijlage 4: Legitimatiekaart



## Bijlage 5: Functieprofiel van een cyberpreventieadviseur

1. Taken
   - ✓ Onder leiding van de coördinator draagt de cyberpreventieadviseur bij tot de ontwikkeling van een geïntegreerd preventiebeleid, in het bijzonder de voorkoming van cybercriminaliteit.
   - ✓ De CPA verleent een advies op maat van de aanvrager. Hij toetst voor de afspraak de noden en vragen af van de burger en legt hier de nadruk op tijdens zijn advies.
   - ✓ De CPA biedt bijstand en ondersteuning tijdens een informatiesessie over cyberpreventie. Dit kan zowel tijdens een buurtvergadering, een opendeurdag, …

2. Functieprofiel
   - ✓ Interesse hebben voor de cyberproblematiek.
   - ✓ Bereid zijn om zich belangeloos in te zetten met de nodige verantwoordelijkheidszin.
   - ✓ Bereid zijn om voldoende tijd te investeren om de opdracht naar behoren te kunnen uitvoeren.
   - ✓ Bereidheid tot het volgen van de opleiding cyberpreventieadviseur en deze opleiding succesvol af te sluiten.
   - ✓ Bereid zijn om op een loyale en vertrouwelijke manier met alle betrokkenen samen te werken en de verkregen informatie discreet te behandelen.
   - ✓ Over voldoende sociale en communicatieve vaardigheden beschikken.
   - ✓ Beschikken over een luisterende houding.
   - ✓ Zowel zelfstandig als in groepsverband kunnen werken.
   - ✓ Flexibel zijn en bereid om ’s avonds (na 18u) en/of op zaterdag huisbezoeken uit te voeren of om presentaties voor groepen te doen.

## Bijlage 6: Inspiratietekst om adviezen te verzamelen

**Wil jij graag tips om je te beschermen tegen cybercriminaliteit?**

Vanaf (datum) stapt de gemeente mee in met het project 'cyberpreventieadviseurs'.
Een cyberpreventieadviseur geeft je enkele nuttige en eenvoudige tips die je beter beschermen tegen online fraude. Zo leert hij je hoe je kan zien of een mail echt of vals is of legt hij het gebruik van tweestapsverificatie uit.
Het is echter niet de bedoeling dat de cyberpreventieadviseur jouw anti-virusprogramma installeert of updatet.

Wil jij graag meer tips om jezelf beter te beschermen tegen cybercriminaliteit? Dan hebben we goed nieuws! Als inwoner kan je vanaf nu cyberpreventieadvies aanvragen via de gemeentelijke website of website van je lokale politie. Vervolgens contacteert de cyberpreventieadviseur jou om af te stemmen wanneer hij bij jou thuis kan langskomen.

Zou je graag als vereniging een cyberpreventieadviseur uitnodigen voor een infoavond voor jouw leden? Ook dit kan! Neem hiervoor contact op met de coördinator via (gegevens contactpersoon gemeente)

Meer info: (gegevens contactpersoon gemeente)

## Bijlage 7: Feedbackdocument – voorbeeld vanuit stad Diest

*Tevredenheidsbevraging cyberpreventieadvies*
*Geachte Heer / Mevrouw,*

*Recent kreeg u advies van een van onze cyberpreventieadviseurs. Graag zouden wij u willen vragen om de volgende enquête in te vullen. Alvast bedankt!*

*Met vriendelijke groeten,*
*Dienst integrale veiligheid stad Diest*

1. Hoe bent u op de hoogte geraakt van de mogelijkheid tot het aanvragen van cyberpreventieadvies?
   - Website stad Diest
   - Lokaal infokrantje
   - Via buren, familie, vrienden
   - Via de politie

2. Waarom heeft u advies aangevraagd?
   - Op aanraden van een buur, vriend, …
   - Online voel ik me onveilig
   - Uit nieuwsgierigheid : Beweeg ik mij veilig online ?
   - Ik wil mee zijn met de ‘digitale sneltrein’
   - Andere : …

3. Bent u tevreden over het cyberpreventieadvies?
   - Ik ben heel tevreden over het cyberpreventieadvies !
   - Ik ben eerder tevreden over het cyberpreventieadvies.
   - Ik ben noch tevreden, noch ontevreden over het cyberpreventieadvies.
   - Ik ben eerder ontevreden over het cyberpreventieadvies.
   - Ik ben eerder ontevreden over het cyberpreventieadvies !
   - Andere : …

4. Lag het advies in de lijn van uw verwachtingen?
   - Ja ! Ga naar vraag 6
   - Nee ! Ga naar vraag 5

5. Hoe dacht u dat het advies er uit zou zien?

6. Was u tevreden over de duur van het advies?
   - Het advies duurde te lang
   - De duur van het advies was perfect
   - Het advies mocht wat langer duren

7. Met welke tips hield jij al rekening voor het advies?
   - Gebruik van een sterk wachtwoord
   - Gebruik van tweestapsverificatie
   - Installeren van een antivirusprogramma
   - Software-update en back-up
   - Open geen berichten en onbekende bestanden die je niet verwacht of niet vertrouwt
   - Controleer het adres (URL) van websites op onregelmatigheden
   - Verbreek het contact met ongevraagde helpdeskmedewerkers
   - Stel je privacyinstellingen zo hoog mogelijk in op sociale media
   - Maak alleen verbinding met vertrouwde wifinetwerken, liefst geen publieke wifi-netwerken

8. Met welke tips ga jij in de toekomst aan de slag?
   - Gebruik van een sterk wachtwoord
   - Gebruik van tweestapsverificatie
   - Installeren van een antivirusprogramma
   - Software-update en back-up
   - Open geen berichten en onbekende bestanden die je niet verwacht of niet vertrouwt
   - Controleer het adres (URL) van websites op onregelmatigheden
   - Verbreek het contact met ongevraagde helpdeskmedewerkers
   - Stel je privacyinstellingen zo hoog mogelijk in op sociale media
   - Maak alleen verbinding met vertrouwde wifinetwerken, liefst geen publieke wifi-netwerken

9. Heeft u nog verdere opmerkingen of aanbevelingen?