# Phishing

**Een e-mail beoordelen: echt of nep?**

CCV centrum voor criminaliteitspreventie en veiligheid

## NOTITIES:

# Phishing?

Van: Jabari [mailto:jabari@btinternet.com]
Verzonden: Vrijdag 23 februari 2018 13:02
Aan: michael.[redacted]@hotmail.com
Onderwerp: [SUSPECT] From Akaoma Chika

Beste vriend,

Ik ben Akaoma Chika, de advocaat en uitvoerder van je overleden familielid, “en” Testament”, die stierf met familie of familieleden van de VN. Ik neem contact met je op om op te treden als nabestaanden van zijn depositofonds van de VS € 9,5 miljoen, met een van de leidende banken hier in West-Afrika, omdat je dezelfde achternaam met hem deelt. De bank heeft me een kennisgeving gestuurd om de nabestaanden te verstrekken.

Gelieve vriendelijk te reageren met de volgende informatie voor verdere verduidelijkingen.

Je volledige naam
Jouw telefoon nummer
Jouw nationaliteit
Je leeftijd.

Ik kijk er naar uit om zo snel mogelijk van je te horen. Als je bereid bent om met mij verder te gaan.

Hoogachtend,
Akaoma Chika.Esq.

CCV centrum voor criminaliteitspreventie en veiligheid

# WAAR LET JE OP:

1. Aanhef: er is geen persoonlijke aanhef.
2. Tekst: er staan overal spelfouten in de tekst.
3. Inhoud: niemand zou zomaar een onbekende een groot bedrag nalaten.
4. Afzender: de afzender komt niet overeen met de ondergetekende.

## Conclusie: deze e-mail is NEP.

Deze e-mail is niet echt en staat bekend als voorschotfraude of 419-fraude. Het slachtoffer krijgt een e-mail waarin wordt aangegeven dat er een groot bedrag is vrijgekomen zoals een erfenis van een zogenaamd (buitenlands) familielid of naamgenoot. Om extra vertrouwen te wekken worden er soms als bijlage echt lijkende certificaten of andere documenten meegestuurd.

Als het slachtoffer reageert op de e-mail, blijkt al snel dat er kosten voor bijvoorbeeld advocaten en administratie gemaakt moeten worden om het geld vrij te krijgen voor de overboeking. In het begin gaat het om kleine bedragen, maar deze lopen vaak snel op. Uiteindelijk blijkt dat er geen geld is en dat het betaalde geld niet meer terugkomt.

# Phishing?

Van: Eneco <no-reply@energie.ru>
Verzonden: donderdag 19 juli 2018 11:44
Aan: suzanne.[redacted]@hotmail.com
Onderwerp: Wat weet jij over Toon, de slimme thermostaat

Beste Suzanne,

Eneco hangt Toon kosteloos aan je muur. Profiteer van Toon met kosteloze installatie t.w.v. vijf-en-zeventig Euro.

Met Toon word je baas over je huis. Met deze slimme thermostaat weet je alles over je energieverbruik en hoe je kunt besparen. Doe mee met deze tijdelijke actie en profiteer van Toon met gratis installatie t.w.v. vijf-en-zeventig Euro.

Wat weet jij over Toon, de slimme thermostaat?

>>Niets, Ik wil graag meer informatie
>>Alles, Ik gebruik Toon thuis zelf

**Wat is Toon?**
De voordelen van Toon

- Weet precies wat je verbruikt. Je weet met Toon precies hoeveel energie je verbruikt. En wat het je kost. Per dag, week, maand of jaar.
- Bespaar op je energierekening. Het inzicht dat Toon je geeft helpt je om bewuster met je energieverbruik om te gaan. Zo bespaar je al snel tot 10% op je energiekosten.

**Bedien je huis op afstand**
Met de kosteloze Toon-app bedien je met je smartphone of tablet de thermostaat ook op afstand. Waar en wanneer je maar wilt.

Houd je cv-ketel in topconditie. Toon stuurt je cv-ketel aan om je huis op temperatuur te houden. Profiteer nog even van deze tijdelijke actie!

>>JA, Ik wil meer informatie
>>NEE Ik heb geen interesse


CCV centrum voor criminaliteitspreventie en veiligheid

# WAAR LET JE OP:

1. Aanhef: er is een persoonlijke aanhef dus dat is een goed signaal.
2. Tekst: er staan geen spelfouten in en de e-mail is netjes opgemaakt.
3. Inhoud: de aanbieding van Eneco klinkt aannemelijk, maar Eneco zal je nooit vragen om op een link te klikken als je geen interesse hebt.
4. Afzender: de afzender van de e-mail is no-reply@energie.ru. Deze extensie is specifiek voor Rusland. Dit zal Eneco nooit gebruiken.

## Conclusie: deze e-mail is NEP.

Deze e-mail is niet echt en is een phishing e-mail. Criminelen proberen de ontvanger op een link te laten klikken. Je wordt dan bijvoorbeeld doorgestuurd naar een malafide website waar malware op je computer wordt geïnstalleerd. Via deze malware kan de crimineel jouw persoonlijke gegevens in handen krijgen. Ook is het mogelijk dat er zogenaamde gijzelsoftware wordt geïnstalleerd waardoor al je computerbestanden worden 'gegijzeld'. Dit heet ransomware. Er moet dan een geldbedrag worden betaald om de bestanden weer vrij te geven.


Ga met je muis over een link en kijk naar welk adres je wordt doorgestuurd. Als je het niet vertrouwt, neem dan eerst telefonisch contact op met de afzender.

# Phishing?

Van: Hendrik-Jan <hendrik-jan@jobseekers.nl>
Verzonden: donderdag 14 juli 2018 18:44
Aan: miriam.[redacted]@ziggo.nl
Onderwerp: Ben je nog beschikbaar?

Jobseekers GROEP BV

Beste Miriam,

Wij hebben in het verleden contact gehad en wij zijn benieuwd naar de status van jouw zoektocht naar een nieuwe baan. Ben jij nog op zoek naar een nieuwe uitdaging, dan helpen wij jou graag in deze zoektocht. Om jou goed te kunnen helpen zouden wij jou willen vragen om jouw meest recente CV naar ons toe te sturen en jouw beschikbaarheid te wijzigen en/of gegevens aan te passen wat kan via de link:

Inloggen op jouw account

Mocht het niet lukken via bovenstaande link dan kun je het ook proberen door de volgende link in je browser te plakken:

https://www.jobseekers.nl/mijnaccount

Naast het updaten van jouw CV kun je ook onze website met de meest recente vacatures in de gaten houden: www.jobseekers.nl. Zie jij hier jouw droombaan tussen staan, aarzel dan niet om ons te contacteren!

Wil jij deze mails liever niet meer ontvangen? Laat dit ons dan weten, dan zorgen wij dat dit geregeld wordt. Mocht je dan in de toekomst toch weer op zoek raken en hier hulp bij willen gebruiken dan kun jij ons natuurlijk altijd benaderen!

Met vriendelijke groet,

Hendrik-Jan de Vries | Jobseekers
Jobseekers Groep BV

# WAAR LET JE OP:

1. Aanhef: er is een persoonlijke aanhef.
2. Tekst: er staan geen spelfouten in en de e-mail is netjes opgemaakt.
3. Inhoud: het recruitingbureau refereert aan een eerder contact. Kun je je dat herinneren? Zo niet, laat de e-mail dan links liggen.
4. Afzender: de afzender van de e-mail komt overeen met de ondergetekende. Het is een duidelijke persoonsnaam bij een domeinnaam en extensie die past bij het bedrijf.

Twijfel je nog steeds? Google dan eens naar de naam van de afzender en bekijk of deze persoon werkzaam is bij het betreffende bedrijf.

Conclusie: deze e-mail is ECHT.

# Phishing?

Van: PostNL <no-reply@nlpost.nl>
Verzonden: 14 juni 2018 05:38:17 CEST
Aan: stefan[redacted]@gmail.com
Onderwerp: **Uw Pakket is onderweg**

## Pakket gemist

Geachte ,
We bezorgen binnenkort een pakket bij u.

**Verwacht bezorgmoment:**
Morgen 15 Juni
10.15 – 14.45 uur

**Afzender: Onbekend**
Barcode: 3SMXXX20232001

Kies een ander moment of plaats

Komt het moment niet uit? Of haalt u het pakket liever af op uw PostNL-locatie?
Wijzig het direct in de Track & Trace.

>>Download Track & Trace

Met vriendelijke groet,
Het team van PostNL



CCV centrum voor criminaliteitspreventie en veiligheid

# WAAR LET JE OP:

1. Aanhef: er is geen persoonlijke aanhef.
2. Tekst: er staan geen spelfouten in en de e-mail is netjes opgemaakt.
3. Inhoud: een bevestiging van het bezorgen van een pakket kan kloppen. Heb je wel iets besteld? Check dan in ieder geval of die afzender staat vermeld. Hier is dat niet het geval. Dit klopt dus niet. Bovendien wordt er gevraagd iets te downloaden. Iets downloaden vanuit een e-mail moet je over het algemeen nooit doen.
4. Afzender: de afzender van de e-mail is no-reply@nlpost.nl. Deze naam lijkt erg op het domein van PostNL maar is net even anders. Dit klopt dus niet.

## Conclusie: deze e-mail is NEP.

Internetcriminelen registreren vaak domeinnamen die lijken op echte bestaande domeinnamen. Op deze manier lijkt het alsof de afzender van de e-mail klopt, zoals in bovenstaand voorbeeld. Zodra je klikt op de downloadlink bestaat de kans dat er malware op je computer wordt geïnstalleerd, waardoor criminelen toegang krijgen tot al jouw persoonlijke gegevens. Of je krijgt te maken met ransomware waardoor al je bestanden worden gegijzeld en je moet betalen om weer toegang te krijgen.

# TIPS

1. **Gebruik sterke wachtwoorden**
   Een sterk wachtwoord is een wachtwoord dat zo lang mogelijk is. Een wachtwoordzin in combinatie met vreemde tekens werkt op dit moment het beste. Kies bijvoorbeeld mijnvrouwheet@)nne&wehebben3KIDS! Maak gebruik van een wachtwoordmanager. Zo hoef je niet zelf voor iedere website het wachtwoord te onthouden.


2. **Log nooit in op openbare wifinetwerken**
   Openbare wifinetwerken zijn over het algemeen niet veilig. Zorg dat medewerkers op hun mobiele telefoon een onbeperkt data abonnement hebben en spreek met elkaar af om onderweg gebruik te maken van dit abonnement op zowel mobiele telefoons als op tablets en laptops.

3. **Zorg voor automatische updates**
   Zorg ervoor dat je altijd instelt dat updates automatisch gedaan worden. Updates en patches zorgen voor optimale beveiliging en herstel van bekende lekken in je software-systemen. Hackers maken veelal gebruik van deze bekende en gepubliceerde lekken.

## TIPS

4. **Breng alle gegevens in kaart**
   Zorg ervoor dat je weet welke gegevens in de organisatie van waarde kunnen zijn voor dieven. Hackers zijn niet altijd alleen maar uit op bankgegevens. Denk ook aan het beveiligen van bijvoorbeeld persoonsgegevens en eventueel octrooien en patenten. Ook in het kader van de AVG ben je verplicht passende maatregelen te nemen om persoonsgegevens voldoende te beveiligen.

5. **Maak altijd back-ups van systemen**
   Als je toch slachtoffer wordt van een cyberaanval kun je altijd terugvallen op deze back-up en je activiteiten voortzetten. Zijn er persoonsgegevens verloren gegaan bij de cyberaanval? Vergeet dan niet om te checken of je verplicht bent melding te maken van een datalek bij de Autoriteit Persoonsgegevens. Test ook op regelmatige basis of de back-ups daadwerkelijk gemaakt worden en teruggezet kunnen worden.

# Phishing?

From: Leon.verver@ccva.nl
Sent: Wednesday, June 06, 2018 8:21 AM
To: Anne.de.winter@ccva.nl
Subject: Dringende betaling

Goedemorgen Anne,

1. Hoeveel is het saldo van onze bankrekening?
2. Kun je vandaag met spoed een internationale betaling verwerken?

Groet,

Leon Verver
Directeur

**CCVA**
Torenstraat 1
3333 AA Deventer
**T** 088 3311444
**E** leon.verver@ccva.nl

CCV centrum voor criminaliteitspreventie en veiligheid

# WAAR LET JE OP:

1. Aanhef: er is een persoonlijke aanhef.
2. Tekst: hier is niets aan op te merken.
3. Inhoud: Leon vraagt wat het saldo is en of er vandaag nog een internationale directe overboeking gedaan kan worden. Let goed op of dit de normale manier is waarop de directeur zou communiceren. Als dat zo is, dan is het goed om voortaan afspraken te maken over verificatie bij ongebruikelijke transacties.
4. Afzender: de afzender van de e-mail is de directeur, dus dat klopt.

## Conclusie: deze e-mail kan NEP zijn.

Ook al lijkt deze e-mail echt afkomstig te zijn van de directeur, in veel gevallen is een dergelijke e-mail nep. Deze vorm van oplichting wordt CEO-fraude genoemd. Meestal gaat het om een internationale overboeking en is er altijd een vorm van haast bij dit soort fraude.

Hackers breken in in het e-mail account van de CEO of vervalsen de afzender van een e-mail (spoofen). Via de website van het bedrijf, LinkedIn of gewoon via de telefoon te vragen naar ‘degene die gaat over overboekingen’ wordt uitgezocht wie verantwoordelijk is voor betalingen. Deze persoon ontvangt dan zogenaamd een e-mail van de CEO met het verzoek een internationale betaling te doen. Zo lijkt het alsof de CEO de opdracht geeft een overboeking te doen. In werkelijkheid stuurt de hacker de betreffende e-mail en verdwijnt de overboeking naar een rekening in het buitenland.

# Phishing?

Van: icscreditcard@marketing.icscards.nl
Datum: maandag 1 oktober 2017 12:01
Aan: [redacted]strik@ziggo.nl
Onderwerp: Wijziging van de spaarrente op uw card

Bekijk de webversie

## Wijziging van de spaarrente op uw Card

Geachte mevrouw Strik,

Bij een positief saldo van € 500,- of meer op uw ABN AMRO Creditcard ontvangt u spaarrente over het totale positieve saldo. Per 15 oktober 2017 wordt de spaarrente die van toepassing is op uw Card gewijzigd van 0,3% naar 0,1% effectief op jaarbasis. Het maximale positieve saldo waarover wij rente vergoeden is € 1.000.000.

**Hoe kunt u sparen op uw Card?**

- Maak het gewenste bedrag over naar uw Card onder vermelding van alleen uw ICS klant-nummer. Uw ICS klantnummer vindt u bovenaan de pagina in Creditcard Online op www.icscards.nl/abnamro en op uw rekeningoverzicht.
- Als het spaarsaldo op uw Card € 500,- of meer bedraagt, ontvangt u automatisch spaarrente. De overboekingen en uw spaarrente worden elke maand op uw rekeningoverzicht vermeld.

**Heeft u vragen?**
Neem dan per e-mail contact met ons op via service@icscards.nl. Als u het niet eens bent met de wijzigingen in het rentepercentage, dan kunt u uw ABN AMRO Credit Card opzeggen. Hiervoor verwijzen we u naar de Algemene Voorwaarden.

Meer informatie over sparen en de Algemene Voorwaarden

Met vriendelijke groet,
International Card Services BV

Uw ABN AMRO Credit Card wordt uitgegeven door International Card Services BV (ICS).

Let op! Ga voorzichtig om met uw persoonlijke gegevens. Medewerkers van ICS zullen nooit naar uw gebruikersnaam, wachtwoord en/of pincode vragen. Niet via e-mail, telefoon of op welke andere manier dan ook.

CCV centrum voor criminaliteitspreventie en veiligheid

# WAAR LET JE OP:

1. Aanhef: er is een persoonlijke aanhef.
2. Tekst: er staan geen spelfouten in en de e-mail is netjes opgemaakt in de huisstijl van ICS.
3. Inhoud: ICS geeft aan dat er een wijziging plaatsvindt op de spaarrente. Op zich zou dit een logische boodschap kunnen zijn. Bedenk wel vooraf of je gebruik maakt van de diensten van ICS voordat je doorklikt. Controleer ook waar de link heen gaat door met je muis over de link heen te gaan zonder te klikken.
4. Afzender: de afzender van de -email is ICScards, dus dat klopt.

Conclusie: deze e-mail is ECHT.

# Phishing?

Van: hans@directverdienen.nl
Verzonden: woensdag 6 juni 2018 08:21
Aan: [redacted].kletten@gmail.com
Onderwerp: vacature

## - Privé en vertrouwelijk -

Hallo meneer / mevrouw,

Wij zijn op zoek naar mensen die op dit moment ons team willen komen versterken. Graag willen we dat je zo snel mogelijk solliciteerd want we zijn erg onder de indruk van jou ervaring.

### We bieden aan:

- Een basissalaris van **€7.550,- per maand**
- Flexibele uren die jou goed uitkomen
- Thuiswerken
- Een goed bonussysteem

Meer informatie over het bedrijf en de vacature is beschikbaar.
**Hier kun je die informatie vinden.**

We raden je aan om zo snel mogelijk te solliciteren
want er zijn slechts een beperkt aantal vrije banen.

**Solliciteer nu.**

Met vriendelijke groeten,

Hans de Groot
Directverdienen.nl

**Nu solliciteren >**

Afmelden doe je nu hier.

CCV centrum voor criminaliteitspreventie en veiligheid

# WAAR LET JE OP:

1. Aanhef: er is geen persoonlijke aanhef.
2. Tekst: er staan spelfouten in.
3. Inhoud: er wordt een aanbieding gedaan om 7500 euro salaris te verdienen met bijzonder gunstige voorwaarden. Over het algemeen kun je stellen dat als iets te mooi lijkt om waar te zijn dit over het algemeen ook zo is.
4. Afzender: de afzender klopt met de ondergetekende.

## Conclusie: dit is een echte e-mail maar pas op!

Deze e-mail zou daadwerkelijk kunnen leiden tot een sollicitatie door middel van bijvoorbeeld Skype. Er wordt door de criminelen een website gemaakt van een nep bedrijf met medewerker profielen die van internet zijn gehaald. Via het interview ontvangen criminelen onder andere persoonsgegevens. Ook komt het voor dat van de medewerker wordt gevraagd om onder het mom van bijvoorbeeld een assessment of integriteitstest grote bedragen op de eigen rekening te ontvangen en dit door te sturen naar een andere rekening. Op deze manier kun je ongewild betrokken zijn bij het witwassen van geld. Je wordt dan ingezet als zogenaamde geldezel. Let dus op als er hoge bedragen als vergoeding worden genoemd en ervoor wordt gezorgd dat je nooit persoonlijk iemand ontmoet.

# Phishing?

Van: info@uwvernieuwde.nl
Datum: 05/02/2018 12:25
Aan: francie.[redacted]@gmail.com
Onderwerp: Introductie vernieuwde bankieren

ING

## Introductie vernieuwde mobiel bankieren

**Geachte ING Rekeninghouder,**

Als klant van de ING wilt u duidelijk en tijdig geïnformeerd worden over veranderingen over onze diensten en producten. We brengen u graag op de hoogte van onze nieuwste ontwikkelingen.

Op basis van feedback van onze klanten ontwikkelen we steeds nieuwe en betere beveiligingssoftware voor het internet bankieren. Door altijd gebruik te maken van de meest recente versie, ervaart u het gemak van de nieuwste functionaliteiten en weet u zeker dat u voldoet aan de laatste veiligheidsstandaarden.

De ING spendeert veel tijd aan het beveiligen van mijn ING, recent heeft de ING een nieuwe beveiligingsupdate ontwikkeld. Naar aanleiding hiervan dient uw rekening geüpdate te worden. Op dit moment maakt u nog geen gebruik van onze vernieuwde omgeving.

Wij betreuren dit omdat u nu niet volop van ons systeem gebruik kunt maken. Momenteel maken we al verschillende stappen om de nieuwe omgeving volledig naar de consument te brengen, zoals met de nieuwe ING Mobiel Bankieren app, die momenteel voor iedereen beschikbaar is. Op dit moment willen wij uw Mijn ING omzetten naar onze nieuwe beveiligde omgeving.

### Mobiel Bankieren

Gemak en veiligheid gaan goed hand in hand. Dat merkt u in de nieuwste versie van de Mobiel Bankieren app. Inloggen zit u letterlijk in de vingers. Als u dat wilt, logt u in en betaalt u met uw vingerafdruk. Snel en simpel. Zoals een overboeking doen, betalen met iDEAL, een beleggingsorder plaatsen en instellingen wijzigen. Zo gaat bankieren in de app nog sneller en eenvoudiger.

We vragen u daarom om uw gegevens te verifiëren, zodra uw gegevens geverifieerd zijn maakt uw automatisch gebruik van onze verbeterde software.

**Mijn ING Online bijwerken >**

### Voordelen van de vernieuwde beveiligingsupdate

De vernieuwde beveiligingsupdate beschikt over verschillende, nieuwe functies waaronder een beveiliging tegen skimming (fraude), meer controle om misbruik van betaalpassen tegen te gaan en zelfs een nieuw systeem die kansen op storingen bijna niet meer mogelijk maakt.

**Voordelen beveiligingsupdate:**

- Vernieuwde beveiliging tegen skimming
- Meer controle door ING personeel
- Versnelde mobiel bankieren koppeling

**Let op:** u dient uw Mijn ING binnen ontvangst van deze mail te updaten. Anders worden uw rekeningen beperkt uit veiligheidsoverwegingen.

Annet van der Hoek
Directeur klantenservice

CCV centrum voor criminaliteitspreventie en veiligheid

# WAAR LET JE OP:

1. Aanhef: er is geen persoonlijke aanhef.
2. Tekst: er staan geen spelfouten in en de e-mail is netjes opgemaakt.
3. Inhoud: het zou kunnen dat ING haar omgeving aanpast en hierover communiceert met haar klanten. Als je geen klant bent, verwijder deze e-mail dan direct. Banken vragen echter nooit om in te loggen via een link in een e-mail. Doe dit alleen via de website of de app van je bank.
4. Afzender: de afzender van de email is info@uwvernieuwde.nl. Dit is geen domein dat ING gebruikt.

## Conclusie: deze e-mail is NEP.

Deze e-mail is niet echt. Internetcriminelen proberen via dit soort e-mails persoonlijke bankgegevens te achterhalen. Zodra je op een link klikt word je doorgeleid naar een website die lijkt op het inlogscherm van de ING. Er kunnen eventueel kleine aanpassingen op de website gemaakt zijn om extra gegevens te achterhalen. Denk hierbij bijvoorbeeld aan het invulveld telefoonnummer. Zodra je inlogt worden de inloggegevens doorgestuurd naar de criminelen. In een telefoongesprek proberen ze een eventuele extra beveiligingscode te achterhalen om vervolgens geld van je rekening te halen.

## NOTITIES:

# KAN IK DEZE E-MAIL VERTROUWEN?

In 7 vragen duidelijkheid over je e-mail

**Heeft de e-mail een persoonlijke aanhef?**
- NEE → Waarschijnlijk is de mail vals!
- JA →

**Lijkt de e-mail foutloos geschreven?**
- NEE → Waarschijnlijk is de mail vals!
- JA →

**Ben je klant bij het genoemde bedrijf?**
- NEE → Waarschijnlijk is de mail vals!
- JA →

**Is de mail verstuurd vanuit een e-mailadres van het bedrijf zelf? @naambedrijf.nl**
- NEE → Waarschijnlijk is de mail vals!
- JA →

**Is de toon van de mail vriendelijk en krijg je voldoende tijd te reageren?**
- NEE → Waarschijnlijk is de mail vals!
- JA →

**Verwijst de mail naar een betrouwbare website?**
- NEE → Plaats de muis boven de link en bekijk welke site achter de link zit zonder te klikken. Werk je met een tablet? Houd dan de link langer ingedrukt.
- JA →

**Wat zegt je gevoel? Is de mail echt?**
- NEE → Mogelijk is de mail vals!
- JA → Waarschijnlijk is de mail echt!

### DE MAIL IS NEP, WAT NU?

Met valse e-mails proberen oplichters gegevens te hengelen (phishing), kwaadaardige software te verspreiden of je een valse rekening te laten betalen. Heb je zo'n mail gekregen? Stuur deze dan door naar valse-email@fraudehelpdesk.nl. Zo help je mee anderen voor de nepmail te waarschuwen. Gooi het bericht vervolgens weg. Heb je geklikt op de mail of gegevens verstrekt? Bel dan met de Fraudehelpdesk op 088 786 7372.

### DE MAIL IS ECHT, WAT NU?

Weet je zeker dat je een echte e-mail hebt gekregen van een bestaand bedrijf? Dan kun je de boodschap natuurlijk niet zomaar negeren. Is de mail vermoedelijk echt, maar twijfel je toch? Neem dan contact op met het bedrijf via de gegevens die je op de website van deze organisatie vindt.

CCV centrum voor criminaliteitspreventie en veiligheid

FRAUDEHELPDESK.nl