Ministerie van Justitie en Veiligheid

# Samen effectief tegen bankhelpdeskfraude

Integrale aanpak
**online fraude**

gezamenlijk opgesteld door:

POLITIE OPENBAAR MINISTERIE nederlandse vereniging van banken vereniging COIN FOX IT part of nccgroup kpn Microsoft

# Samen effectief tegen bankhelpdeskfraude

Bankhelpdeskfraude is een groot maatschappelijk probleem. In 2022 werden slachtoffers in Nederland voor 51 miljoen euro opgelicht door fraudeurs[1]. Sommige mensen worden meerdere malen slachtoffer van een fraudeur die zich voordoet als een medewerker van een bank. Dat moet stoppen. Eind 2020 besloot de overheid op aandringen van de Tweede Kamer tot de integrale aanpak online fraude. De integrale aanpak is een publiek-private samenwerking om het aantal slachtoffers van online fraude te verminderen.[2] De focus van de integrale aanpak online fraude ligt op diverse online fraudevormen, waaronder bankhelpdeskfraude.

## Criminal journey

Politie[3], Openbaar Ministerie (OM), banken[4], Telecom[5], Microsoft en Fox-It hebben, onder begeleiding van Ernst & Young Forensic & Integrity Services (EY), nauw samengewerkt om de reis van de crimineel (de 'criminal journey') bij bankhelpdeskfraude in kaart te brengen en barrières in beeld te brengen en op te werpen. Deze criminal journey laat zien welke zes fasen een crimineel doorloopt bij bankhelpdeskfraude. Met de criminal journey als basis hebben de samenwerkende partijen vervolgens een barrièremodel ontwikkeld. Dit model laat per fase zien welke barrières de verschillende partijen kunnen opwerpen tegen bankhelpdeskfraude.

## Bankhelpdeskfraude

De deelnemende partijen benadrukken het belang dat iedere organisatie zijn eigen rol en verantwoordelijkheid binnen de fraudeketen kent en neemt. Private partijen zoals e-commerce, internet serviceproviders, telecom, social mediaplatforms en banken dragen elk de verantwoordelijkheid om maatregelen te nemen als hun product of dienst wordt misbruikt door fraudeurs. Ook publieke partijen hebben een belangrijke taak om fraude te bestrijden. Ten slotte is het van belang dat consumenten zich bewust worden van de risico's zodat ze geen geld overmaken of waardevolle spullen afgeven aan fraudeurs.

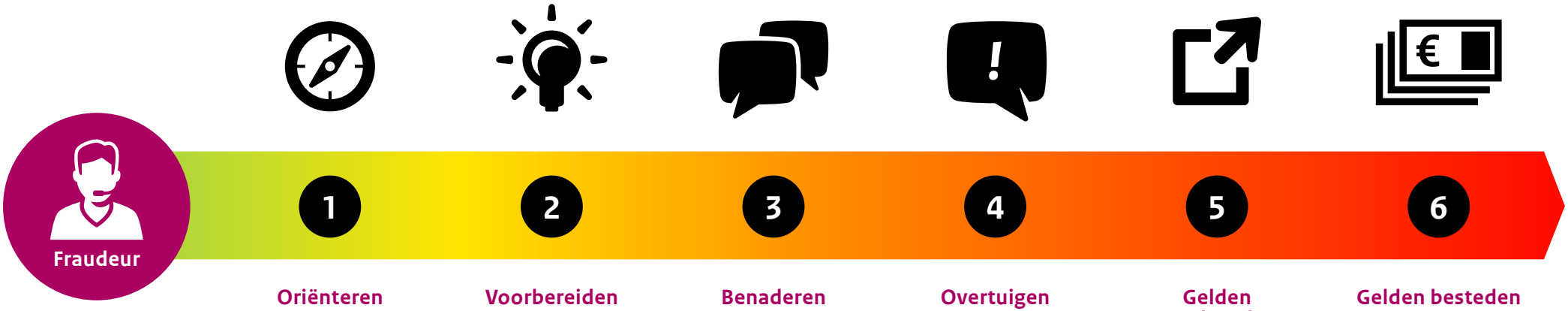
## Maatregelen

De criminal journey en het barrièremodel stellen partners in staat om passende maatregelen te treffen om bankhelpdeskfraude zo veel mogelijk tegen te gaan. Politie en OM werken aan concrete acties om slachtoffers te voorkomen, daders te verstoren, op te sporen en te vervolgen. Het ministerie van Justitie en Veiligheid zet zich in om sociale mediaplatforms verantwoordelijk te houden voor frauduleuze content. Banken onderzoeken, naast de reeds bestaande maatregelen, nieuwe mogelijkheden om slachtoffers zoveel mogelijk te voorkomen en de schade te beperken. En ook Telecom en Microsoft onderzoeken verdere ondersteunende maatregelen ter bestrijding van bankhelpdeskfraude.

Deelnemende partijen zijn zich bewust van hun rol en mogelijkheden binnen de fraudeketen en nemen de bijbehorende verantwoordelijkheid. Bij deze roepen de deelnemende partijen andere partijen binnen de fraudeketen op om ook maatregelen te nemen om het aantal slachtoffers van bankhelpdeskfraude te verlagen en bankhelpdeskfraude te voorkomen. Samen staan we sterker!

1. Veiligheid - Nederlandse Vereniging van Banken (NVB) (bankinbeeld.nl)
2. Aangesloten partners zijn o.a. de politie, het Openbaar Ministerie, VNO-NCW/MKB Nederland, Vodiom, Consumentenbond, NVB, COIN (telecomsector), Thuiswinkel.org, Meta (facebook, WhatsApp), VNG en de ministeries van EZK, Financiën en Justitie en Veiligheid.
3. Waaronder de Electronic Crimes Task Force (ECTF).
4. Nederlandse vereniging van banken, ABN AMRO Bank N.V., ING, Volksbank, Rabobank, Triodos, Knab en Nationale Nederlanden (financiële dienstverlener).
5. Vereniging COIN (Vereniging voor Telecomaanbieders) en KPN B.V.

# Criminal Journey Bankhelpdeskfraude




### 1 Oriënteren

De fraudeur verzamelt informatie over bankhelpdeskfraude, modus operandi en potentiële slachtoffers

### 2 Voorbereiden

De fraudeur verhult zijn/haar (online) identiteit en zorgt ervoor dat ondersteunende middelen voor bankhelpdeskfraude aanwezig en ingesteld zijn

### 3 Benaderen

De fraudeur legt (telefonisch) contact met potentiële slachtoffers

### 4 Overtuigen

De fraudeur overtuigt potentiële slachtoffers dat hun gelden en eigendommen snel veiliggesteld moeten worden

### 5 Gelden overhevelen

De fraudeur bemachtigt de benodigde gegevens van slachtoffers en brengt de gelden en eigendommen buiten de beschikkingsmacht van de slachtoffers

### 6 Gelden besteden

De fraudeur besteedt de vanuit misdrijf verkregen gelden, sluist de gelden door naar andere kanalen of verkoopt de eigendommen