

Gespreksnotitie bestrijding van online fraude

Dr. Susanne van 't Hoff-de Goede, associate lector cybercrime & cybersecurity, de Haagse Hogeschool

In 2024 werden 1,4 miljoen Nederlanders online opgelicht.¹ De impact is vaak groot, waarbij de gerapporteerde mentale gevolgen geregeld groter zijn dan de financiële. Fraudeurs gaan zo gewiekst te werk, dat iedereen slachtoffer van online fraude kan worden.² Dit beeld is niet nieuw en komt al jaren naar voren in onderzoek. Toch worden er nog veel te weinig stappen gezet om online fraude terug te dringen en burgers te beschermen. Wetenschappelijk onderzoek wijst op diverse mogelijke stappen:

1. Preventie.

a. Gericht op slachtoffers.

Een van de grootste risicofactoren voor slachtofferschap van fraude is eerder slachtofferschap.² Slachtoffers van online fraude lopen (veel) meer risico dan anderen om opnieuw slachtoffer te worden, van hetzelfde of een ander delict. Hoewel er meer onderzoek nodig is om dit te verklaren, zou er reeds ingezet moeten worden op de ontwikkeling van wetenschappelijk onderbouwde preventieve interventies gericht op herhaald slachtofferschap.

b. Gericht op potentiële slachtoffers.

- Fraudeurs lichten mensen op door middel van “social engineering”. In vele vormen van fraude worden dezelfde manipulatie technieken gebruikt. Voorkom fraude door mensen weerbaar te maken.
- Hierbij is het van groot belang dat interventies en campagnes die zich richten op gedragsverandering verder gaan dan het vergroten van awareness. Meer kennis leidt niet automatisch tot veiliger gedrag.³
- Zet in op digitale geletterdheid en weerbaarheid in het onderwijs en daarbuiten.

c. Gericht op de systemen en het betaalverkeer.

Interventies gericht op het gedrag van (potentiële) slachtoffers zullen nooit afdoende zijn. Er moet worden ingezet op technische maatregelen tegen online fraude. Bescherm internetgebruikers tegen fraude door bijvoorbeeld systemen te beveiligen met *security by design* of het waar mogelijk tegengaan van anoniem betaalverkeer.

d. Gericht op daders en criminele netwerken.

Zet bijvoorbeeld in op preventie van geldezelen en (vroege) preventie van online crimineel gedrag.

¹ CBS (2025). Online Veiligheid en Criminaliteit 2024.

² Zie voor een overzicht van de literatuur: Van 't Hoff-de Goede, S. & R. Leukfeldt (2024). Slachtofferschap van cybercriminaliteit. In W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (eds.) *Basisboek Cybercriminaliteit*. P. 229-255. Boom Criminologie.

³ Van 't Hoff-de Goede, S., van der Kleij, R., van de Weijer, S., & Leukfeldt, R. (2019). Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders. *Den Haag: WODC, De Haagse Hogeschool, NSCR*. Beschikbaar via <https://repository.wodc.nl/handle/20.500.12832/2433>

- e. Interventies moeten wetenschappelijk worden onderbouwd en geëvalueerd. Maak gebruik van de kennis die er al is, zet onderzoekers in bij het evalueren en zet in op evidence based doorontwikkeling.
2. Zorg voor slachtoffers.
- a. Elke Nederlander moet weten wat te doen in geval van fraude. Veel Nederlanders kennen de eerste belangrijke stap nog niet: bel je bank. Ook zijn ze vaak onbekend met het noodnummer dat ook buiten kantooruren bereikbaar is. Pas als dit algemeen bekend is en slachtoffers zich daadwerkelijk hier melden, kunnen betaaldienstverleners waar mogelijk ingrijpen, en vervolgens slachtoffers doorverwijzen naar (hulp)organisaties voor hulpverlening, aangifte en/of registratie.
 - b. Er is een breed scala van organisaties die klaarstaat voor slachtoffers. Dit heeft als ongewenst neveneffect dat slachtoffers niet altijd weten waar ze het beste terecht kunnen (door de bomen het bos niet zien als je online zoekt naar hulp en informatie). De keten van partijen moet niet alleen samenwerken, maar ook samen optreden richting slachtoffers. Dit zou bovendien behoefte-gestuurd moeten worden aangeboden. Behoeften van slachtoffers lopen namelijk (sterk) uiteen.²
 - c. Een mogelijke route naar genoegdoening voor slachtoffers van online fraude loopt via het civiel recht, waarbij slachtoffers het verloren geld terugvorderen van de ontvanger van het geld. Een grootschalig onderzoek wordt momenteel uitgevoerd door mijzelf en collega Merel van Leuken naar de werking en gevolgen van deze aanpak van online fraude. Diverse deelrapporten zijn openbaar,⁴ de eind-publicatie volgt in 2026.
 - d. Overweeg vergoeding voor slachtoffers vanuit een fonds of betaaldienstverleners. Leer van buitenlandse voorbeelden, zoals de vergoeding die banken in het VK hebben ingevoerd in 2024.
3. Zicht op fraude.
- a. Voor de aanpak van online fraude is inzicht nodig. Hiervoor moet de meldingsbereidheid van slachtoffers worden vergroot. De niet-melders moeten ook worden bereikt en indien gewenst doorverwezen.
 - b. Een van de redenen dat slachtoffers niet melden of hulp zoeken is victim blaming.² Zo geven bekenden slachtoffers de schuld en ook professionals reageren geregeld verwijtend. Bovendien geven slachtoffers zichzelf ten onrechte de schuld van wat hen is overkomen. Dit vergroot niet alleen de impact, maar verkleint ook de bereidheid om te melden en hulp te zoeken.

Er is veel meer wetenschappelijk onderzoek nodig naar slachtofferschap en weerbaarheid van online fraude. Het onderzoeksprogramma “weerbaar tegen online criminaliteit”⁵ zal zich de komende jaren richten op diverse bovenstaande thema’s. Dit programma wordt uitgevoerd door de Haagse Hogeschool en Hogeschool Saxion en wordt mogelijk gemaakt door Fonds Slachtofferhulp en het Ministerie van J&V.

⁴ <https://www.dehaagsehogeschool.nl/onderzoek/centres-expertise/civielrechtelijke-afdoening-van-online-fraude>

⁵ <https://fondsslachtofferhulp.nl/nieuws/onderzoeksprogramma-online-criminaliteit/>