

Een onderzoek door Stemmingmakers

Online oplichting en jongeren: een inkijk in hun ervaringen



Een onderzoek naar de ervaringen van middelbare scholieren met online oplichting en cybercrime.



Inleiding

Aanleiding

Samen met het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV) werken we al een aantal jaar aan een doorlopende preventiecampagne voor jongeren, om hen te waarschuwen voor en informeren over online oplichting.

Het online landschap verandert echter snel en jongeren lopen vaak voorop in die ontwikkelingen. In 2017 hebben we voor het laatst uitgevraagd wat de ervaringen van jongeren zijn met online oplichting. Om de nieuwe preventiecampagne optimaal te laten aansluiten bij de belevingswereld van jongeren, vonden we het belangrijk om opnieuw de ervaringen, het gedrag en de houding ten opzichte van online oplichting in kaart te brengen..

Onderzoeksopzet & methode

Op basis van de vragenlijst van het onderzoek uit 2017, hebben we samen met experts van het CCV een nieuwe vragenlijst opgesteld. De vragenlijst bestaat deels uit dezelfde vragen als in 2017 en deels uit nieuwe vragen. We hebben daarnaast ook een aantal stellingen toegevoegd, om meer inzicht te krijgen in de houding van jongeren ten opzichte van online oplichting en online veiligheid. De vragenlijst (toegevoegd als bijlage) bestaat uit 15 inhoudelijke vragen en een aantal vragen over de achtergrondkenmerken van de deelnemers. Er wordt gebruik gemaakt van routing, dus deelnemers krijgen alleen de vragen te zien die voor hen relevant zijn.

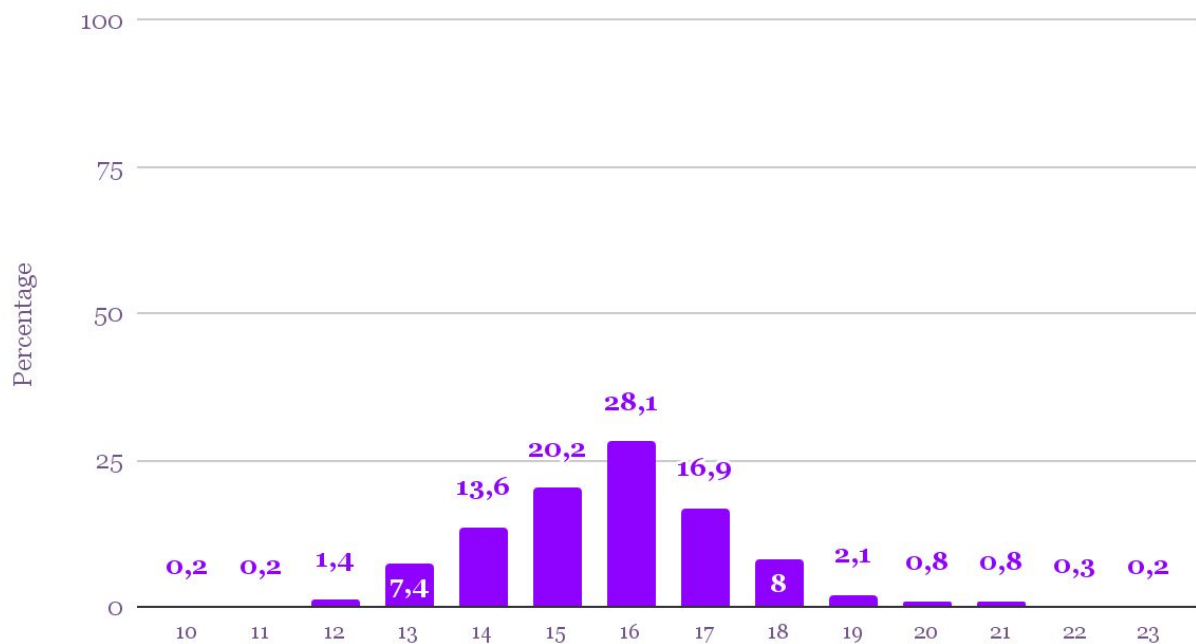
Tussen 20 juni en 8 juli 2024 is de online vragenlijst verspreid via een mailing naar de leden van het jongerenpanel die in de doelgroep vallen en een oproep op de website Scholieren.com.

658 respondenten hebben de vragenlijst ingevuld. Na het verwijderen van niet bruikbare reacties, bleven er **634** geldige responses over. De onderzoeksresultaten zijn gebaseerd op dit aantal respondenten. De resultaten zijn niet volledig representatief voor alle middelbare scholieren in Nederland en kunnen het best beschouwd worden als een peiling.

Steekproef- samenstelling

Demografische gegevens

Leeftijd

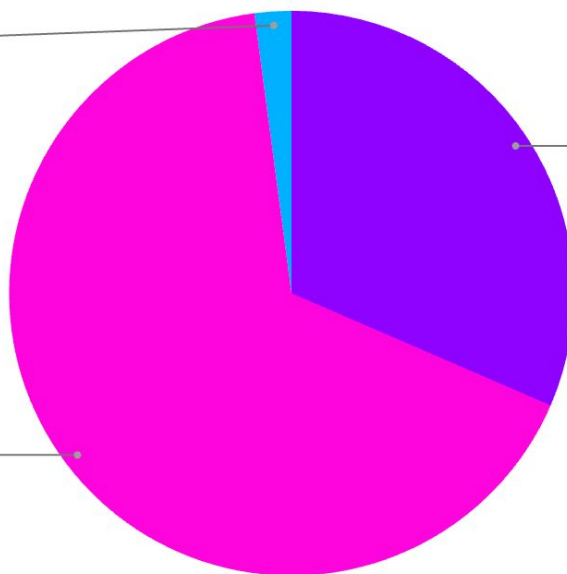


Geslacht

Non-binair
2,1%

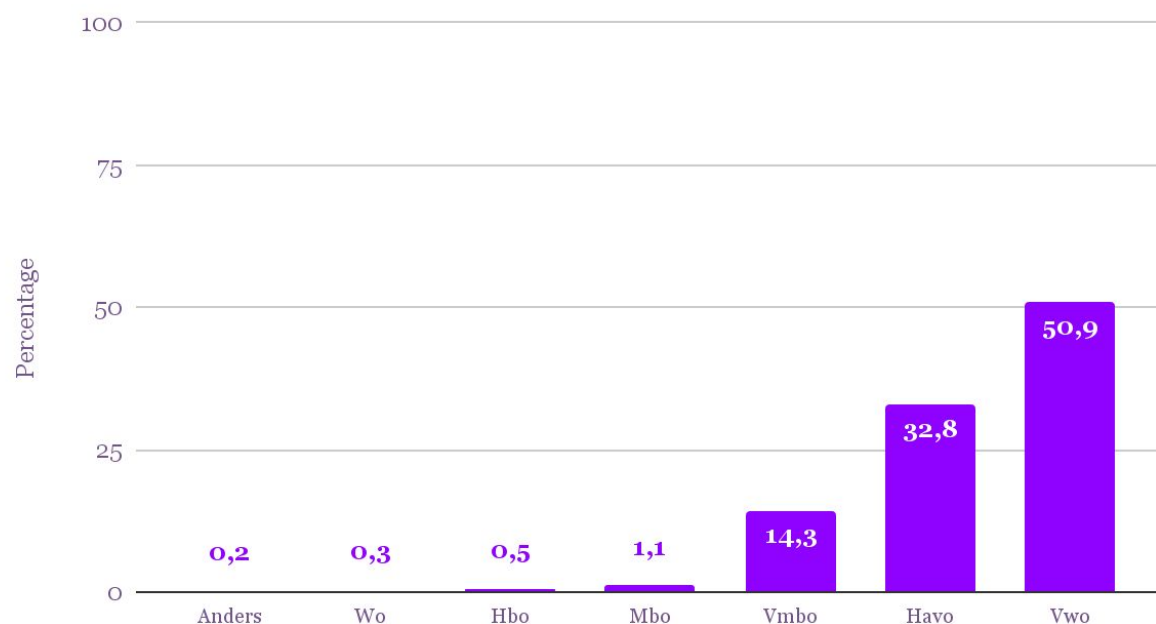
Vrouw
66,4%

Man
31,5%

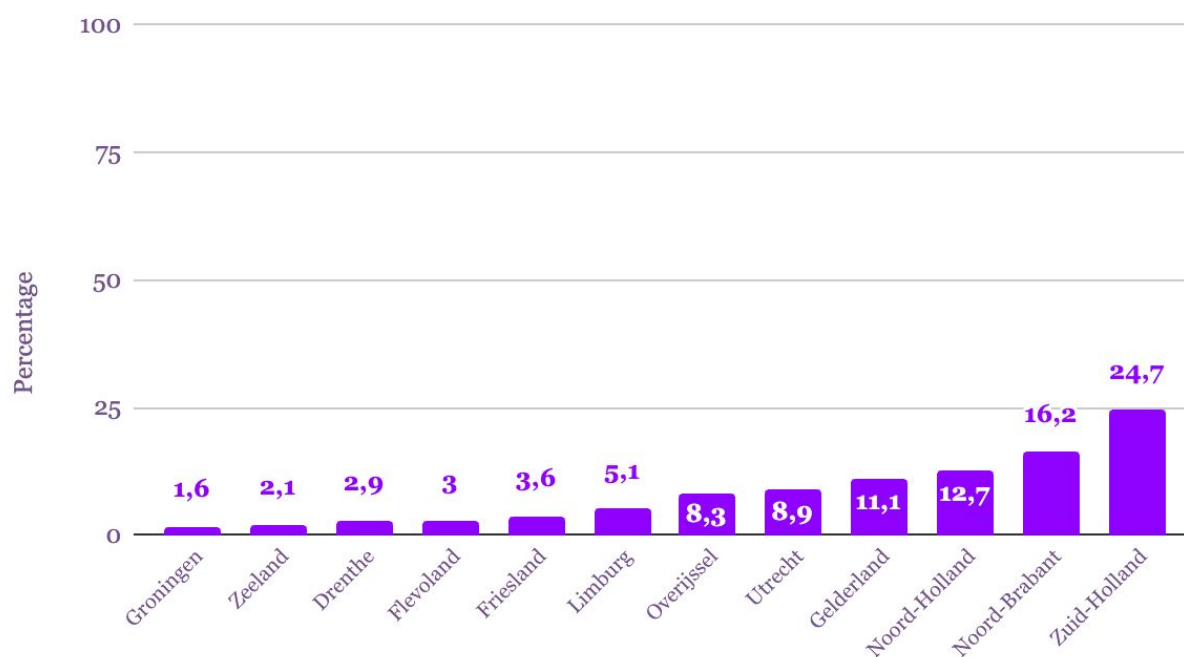


Demografische gegevens

Opleidingsniveau



Provincie

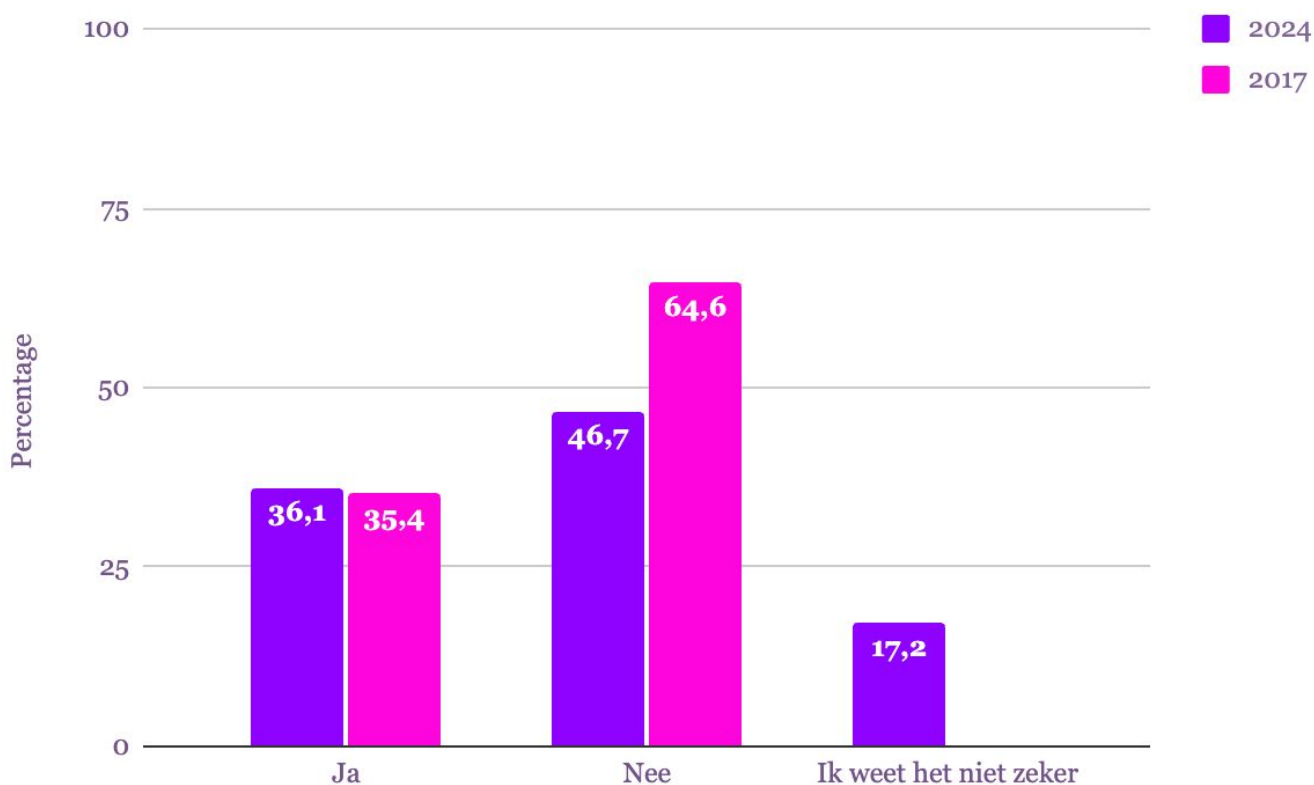


Resultaten

Ervaringen met online oplichting.

Ervaring met oplichting

Ben jij wel eens opgelicht?

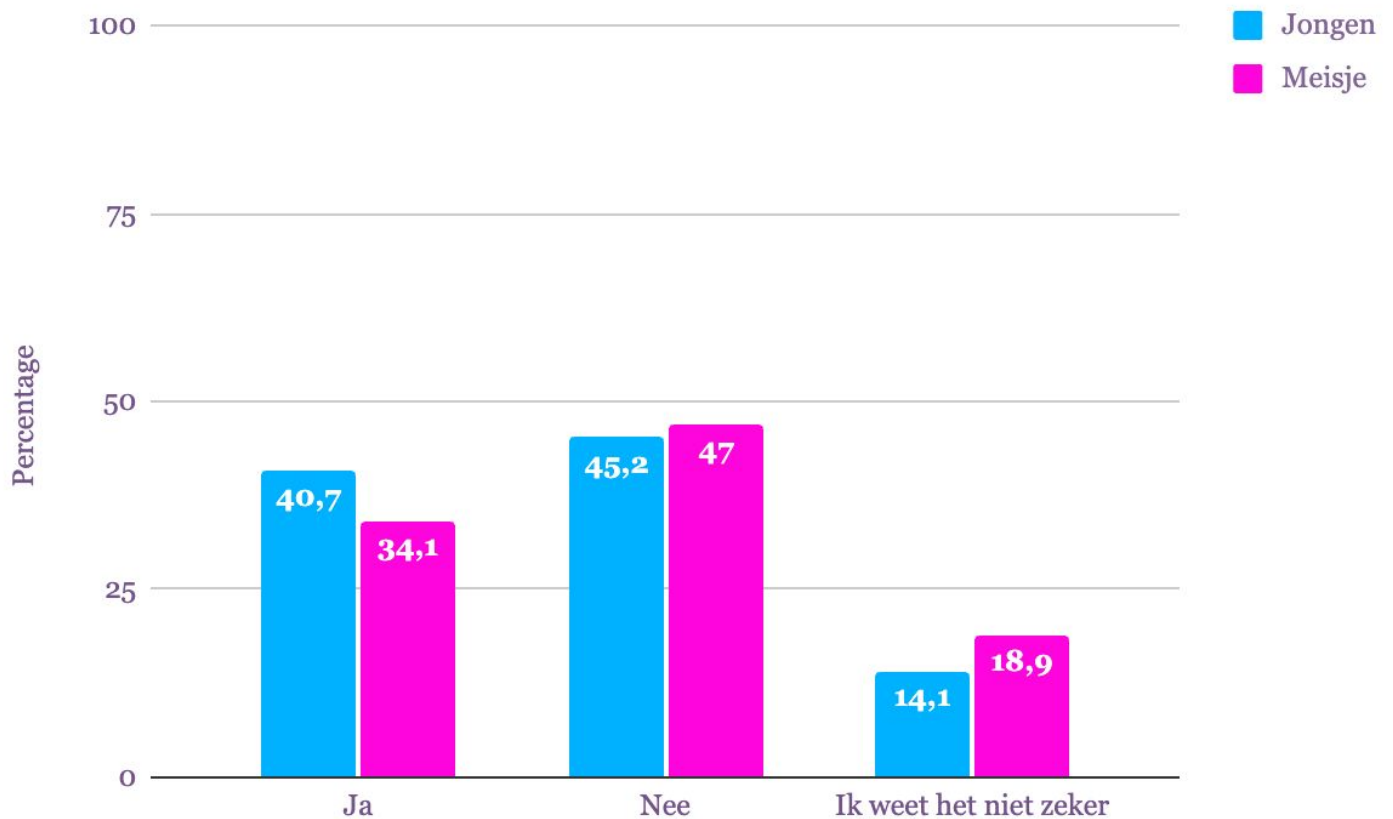


Interpretatie

Ruim een derde van de respondenten geeft aan weleens online opgelicht te zijn. Een groep van ruim 17 procent weet niet zeker of hetgeen ze meegemaakt hebben onder oplichting valt. Als we deze cijfers vergelijken met 2017, het jaar waarin we dezelfde vraag voorgelegd hebben aan middelbare scholieren, zien we dat het percentage scholieren dat naar eigen zeggen online is opgelicht heel licht gestegen is. 'Ik weet het niet zeker' was in 2017 geen antwoordoptie.

Ben jij weleens opgelicht?

Uitsplitsing op basis van geslacht.

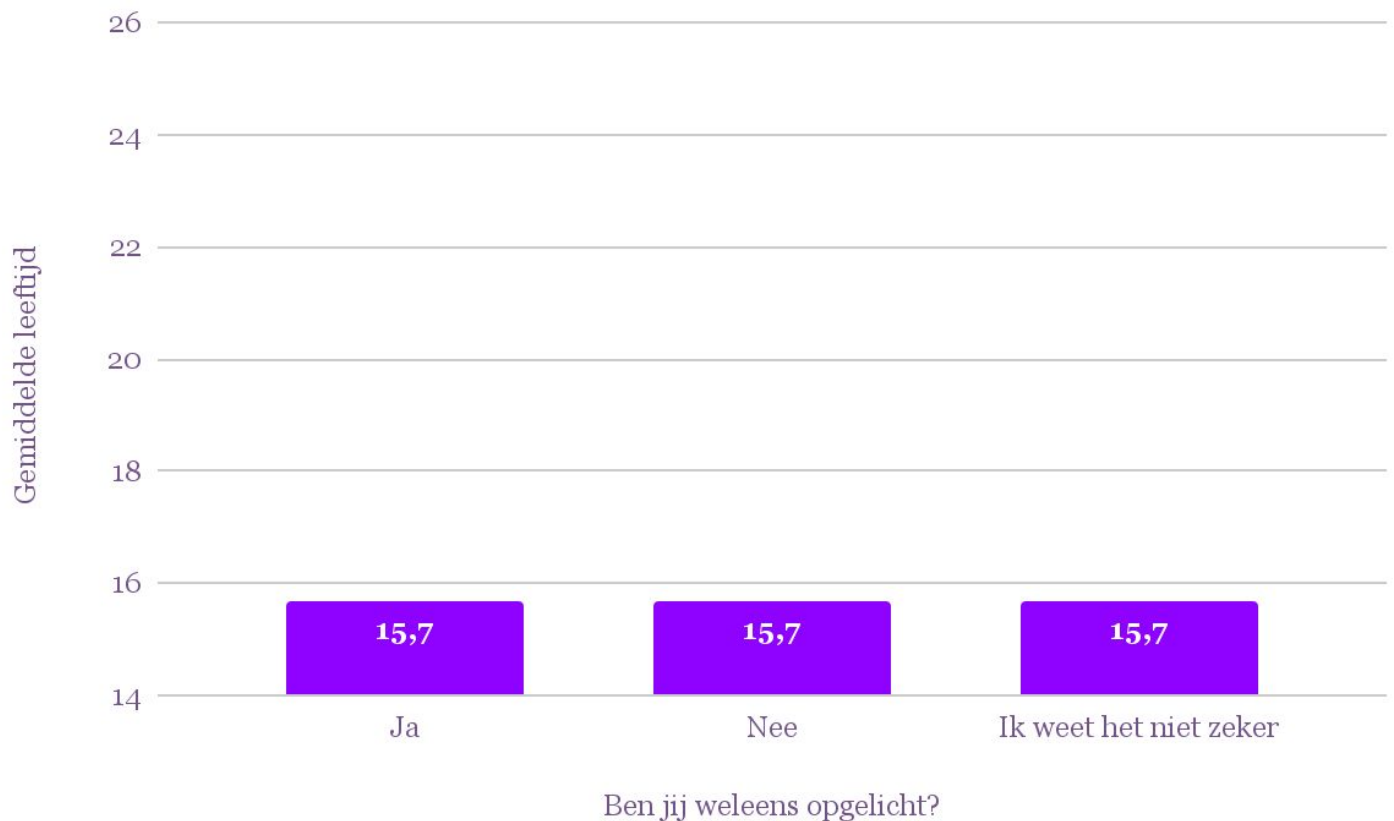


Interpretatie

Uit de resultaten blijkt dat jongens vaker volmondig 'ja' antwoorden op de vraag of zij weleens zijn opgelicht. Meisjes twijfelen hier vaker over en kiezen meer voor 'ik weet het niet zeker'. De percentages van de respondenten die zeggen niet te zijn opgelicht, zijn vrijwel gelijk.

Ben jij weleens opgelicht?

Uitsplitsing op basis van van leeftijd.



Interpretatie

De gemiddelde leeftijd van de respondenten die wel zeggen te zijn opgelicht, verschilt niet van de gemiddelde leeftijd van de mensen die niet zijn opgelicht.

Hoe ben je (volgens jou) opgelicht? En door wie of wat?

Deze vraag is gesteld aan de respondenten die wél opgelicht zijn.

Aan de 36,1% van de respondenten die naar eigen zeggen wel eens is opgelicht, is gevraagd hoe dat is gebeurd en door wie of wat. In een groot deel van de antwoorden komen voorbeelden terug van aankoopfraude via webwinkels, Marktplaats en in iets mindere mate Vinted. In sommige gevallen is het overigens niet duidelijk of er daadwerkelijk sprake is van oplichting of fraude, maar wordt het dus wel als zodanig ervaren door jongeren.

“We hadden zwembad gekocht en hij is nooit binnen gekomen. Later ontdekten we op een fraudesite dat deze site inderdaad nep was.”

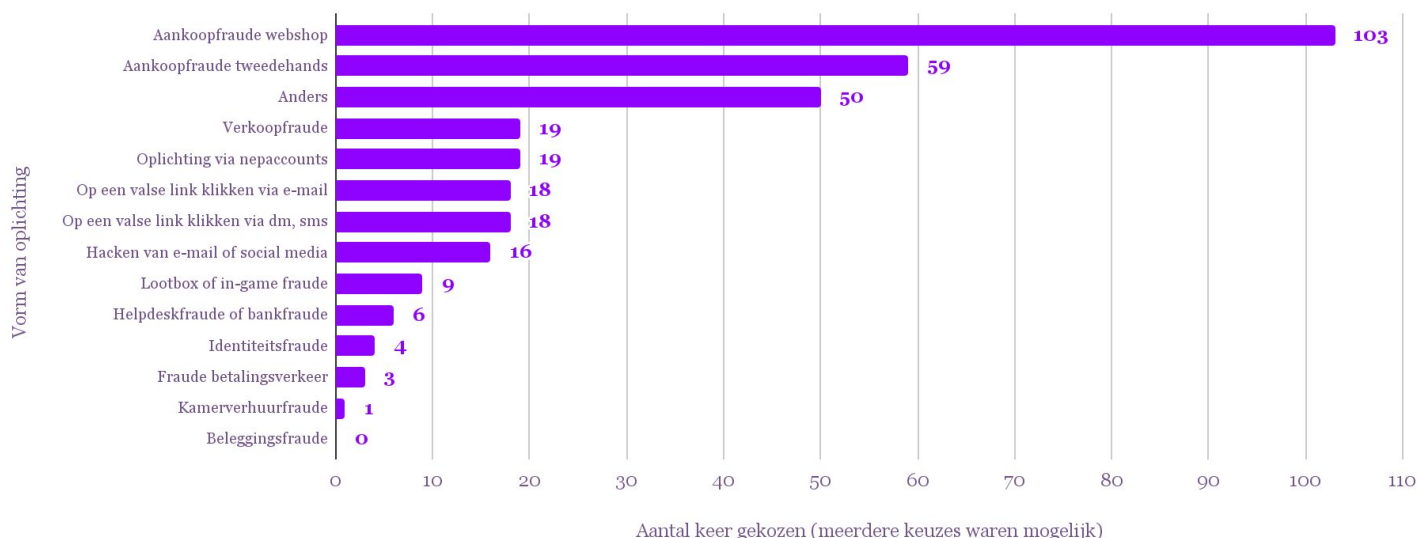
“Ik had 3 rokjes besteld. Ik zag het op TikTok en heb het nooit binnen gekregen.”

Daarnaast worden er ook andere vormen van oplichting benoemd, die minder vaak voorkomen.

“Ik ben opgelicht door een man die zei dat hij mijn broer was en dat hij snel geld nodig had voor een nieuwe telefoon.”

Het komt ook voor dat men vaag is in de beschrijving van wat er precies gebeurd is. Zo vermeldt een respondent bijvoorbeeld dat er ‘geld van zijn bankrekening is gehaald’. En een andere reactie: ‘ik ben opgelicht doordat het account van een van mijn vrienden gehackt was’. Wat er precies gebeurd is, blijft dan onduidelijk.

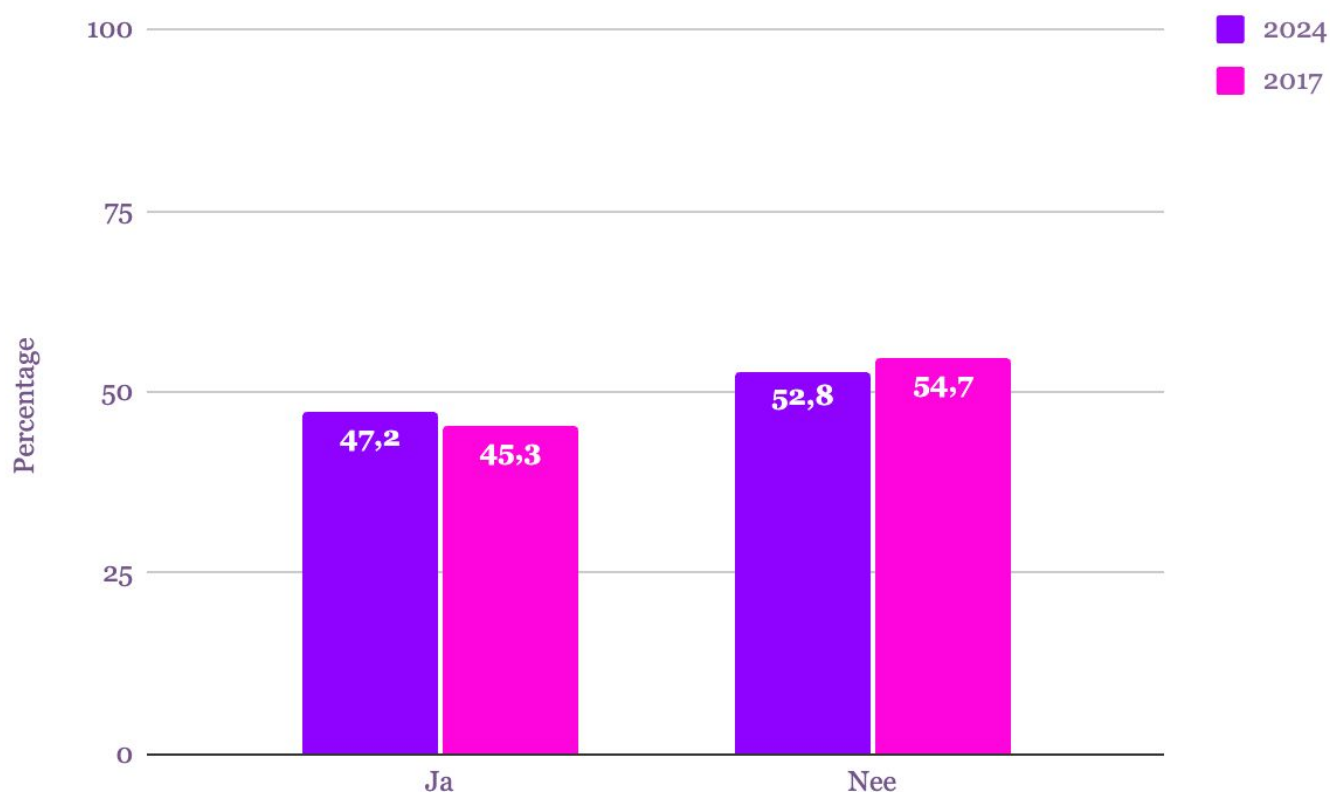
Welke omschrijving van oplichting past het best bij jouw ervaring?



Interpretatie

Als aan respondenten die naar eigen zeggen online zijn opgelicht gevraagd wordt bij welke vorm van oplichting hun ervaring het best past, dan wordt 'aankoopfraude via een webshop' het meest genoemd. Ook 'aankoopfraude via een tweedehands marktplaats' scoort hoog. Daarnaast is er een aanzienlijke groep die hun ervaring als 'anders' aanmerken. Hier vinden we voornamelijk reacties van respondenten die online iets besteld hebben wat wél bezorgd is, maar niet aan de verwachting voldoet of niet teruggestuurd kon worden. Dit valt overigens niet noodzakelijkerwijs onder online oplichting.

Is één van jouw vrienden weleens opgelicht?



Interpretatie

Bijna de helft van de respondenten geeft aan dat een van hun vrienden online weleens is opgelicht. Dit percentage is ook licht gestegen ten opzichte van 2017.

Hoe was hij/zij opgelicht? En door wie of wat?

Aan de 47,2% van de respondenten van wie een vriend of vriendin weleens is opgelicht, is gevraagd hoe dat is gebeurd en door wie of wat. We zien hier een vergelijkbaar beeld in de antwoorden. Opnieuw geeft een groot deel van de respondenten aan dat het ging om aankoopfraude via webwinkels, Marktplaats en in iets mindere mate Vinted.

“Ze wilde een pakketje bestellen en had het geld overgemaakt via Instagram DM. Een dag later was het account verdwenen.”

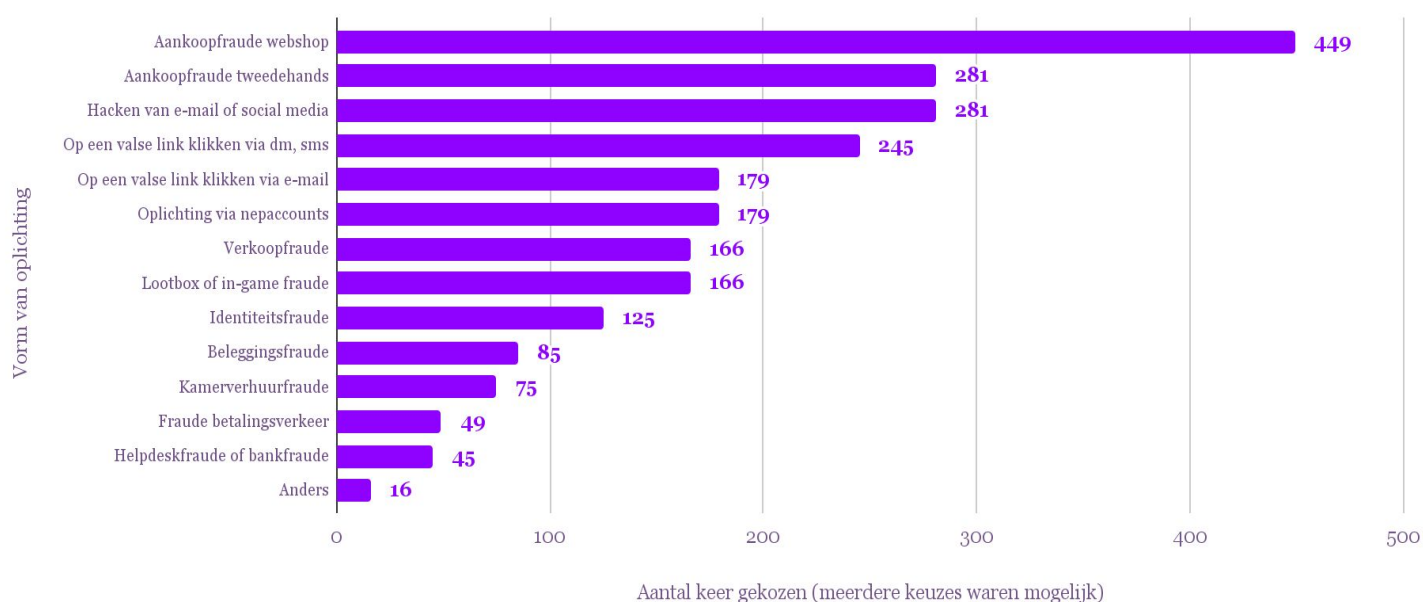
Daarnaast worden er ook andere type oplichting benoemd, die minder vaak voorkomen, bijvoorbeeld oplichting via gaming of het hacken van accounts.

“In een game, hij had digitaal geld uitgegeven in het spel en kreeg vervolgens niet de dingen die hij had gekocht voor in de game.”

“Door iemand die zich voordeed als familielid, en om geld vroeg omdat ze in nood was. Dat familielid had ook nog een jong kind waardoor het erger was als hij niet betaalde.”

De overige antwoorden lopen sterk uiteen en worden niet altijd uitvoerig of duidelijk beschreven.

Van welke vormen van online oplichting worden jongeren het makkelijkst slachtoffer, denk jij?



Interpretatie

Als we aan de respondenten vragen van welke vorm van online oplichting zij denken dat jongeren het makkelijkst slachtoffer worden, scoort aankoopfraude wederom het hoogst. Ook het hacken van een e-mail of social media-account wordt veel genoemd en het klikken op een valse link via dm, sms, WhatsApp of via e-mail (phishing).

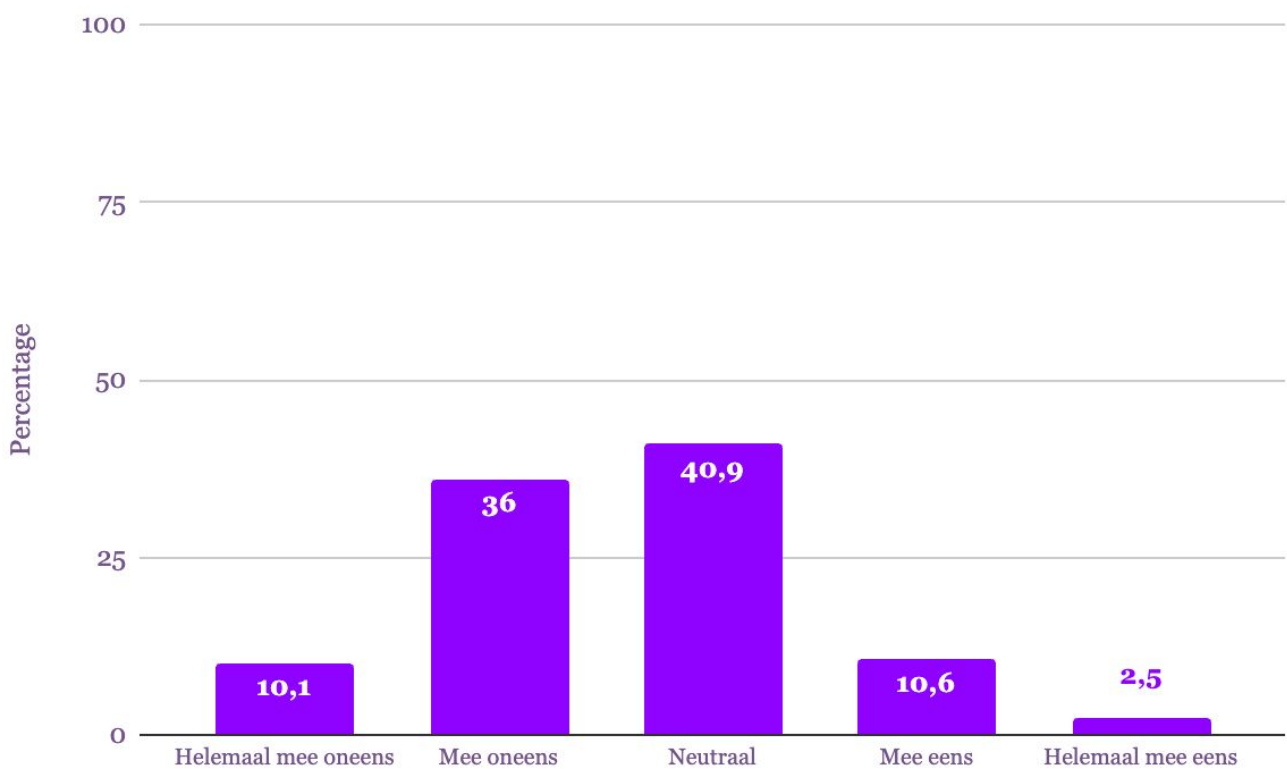
Als we deze resultaten vergelijken met de resultaten van de vraag waarbij jongeren die zijn opgelicht moesten kiezen welke omschrijving het best bij hun ervaring paste (pagina 12), dan zien we dat 'aankoopfraude webshop' en 'aankoopfraude tweedehands' daar ook de top-2 vormen. Daarnaast zien we dat jongeren verwachten dat ze vatbaar zijn voor 'hacken van e-mail of social media account' en 'op een valse link klikken', maar dat dit iets minder vaak gerapporteerd werd als ervaring.

Resultaten

Houding ten opzichte van online oplichting.

Houding online oplichting

Als je online wordt opgelicht, is dat je eigen schuld.



Interpretatie

Bijna de helft van de respondenten vindt het niet je eigen schuld als je online wordt opgelicht. Ook ruim 40% staat hier neutraal in. De gemiddelde score is 2,57.

Als je online wordt opgelicht, is dat je eigen schuld.

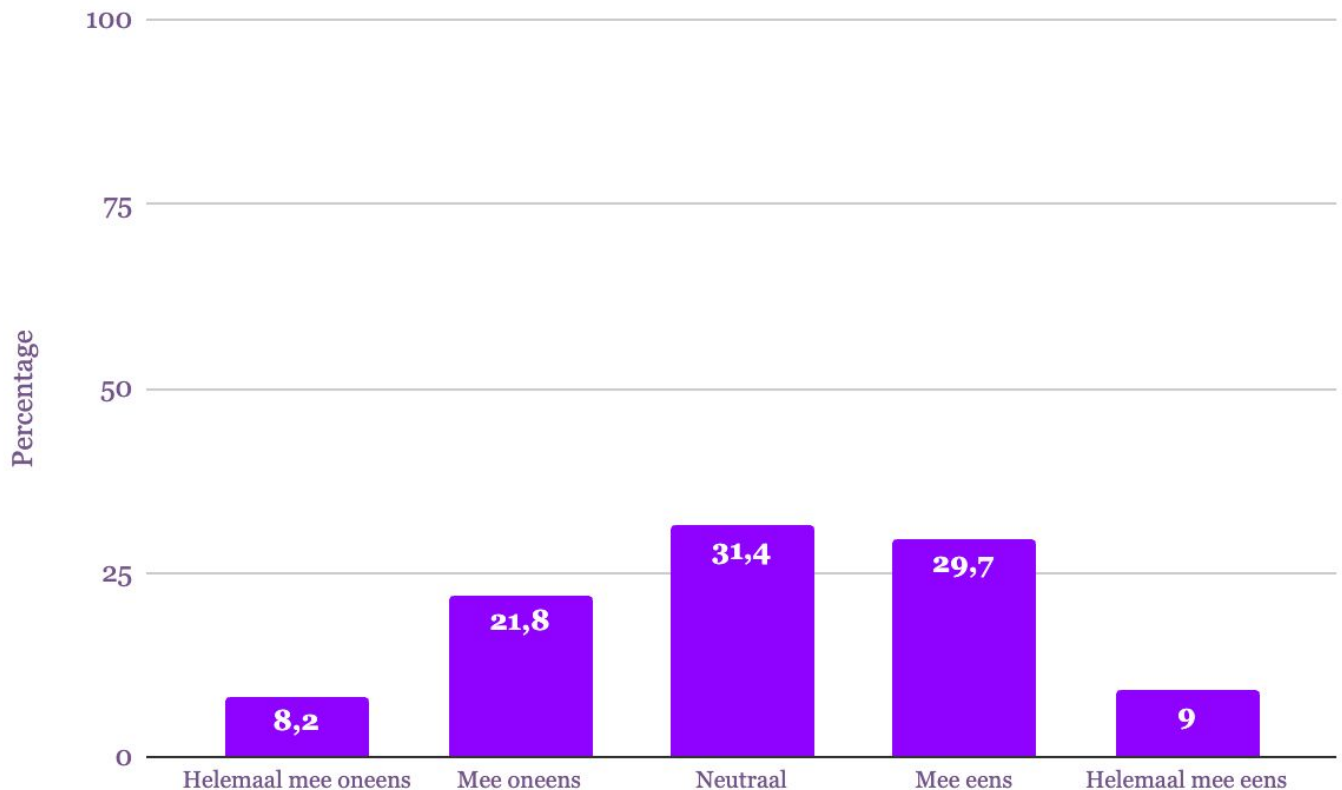
Uitsplitsing op basis van wel/niet zelf opgelicht.



Interpretatie

De groep respondenten die zelf **niet** is opgelicht, scoort een klein beetje hoger op deze stelling, wat betekent dat deze groep het iets vaker je eigen schuld vindt als je wordt opgelicht. De verschillen zijn echter heel erg klein.

De kans is klein dat ik zelf slachtoffer word van online oplichting.

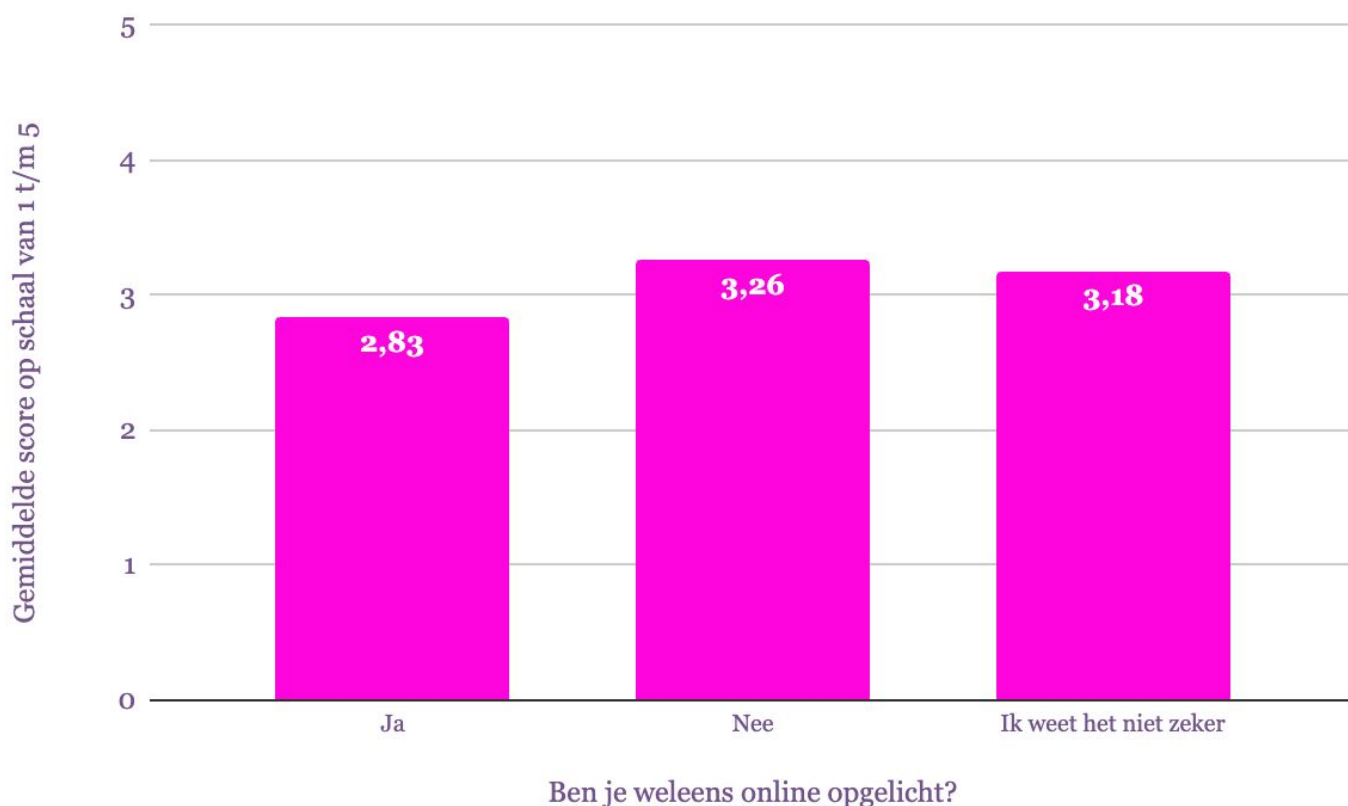


Interpretatie

Bijna 40% van de respondenten schat de kans dat zij zelf slachtoffer worden van online oplichting klein in. Ongeveer een derde van de respondenten staat er neutraal in en nog ongeveer een derde denkt dat die kans wél groot is.

De kans is klein dat ik zelf slachtoffer word van online oplichting.

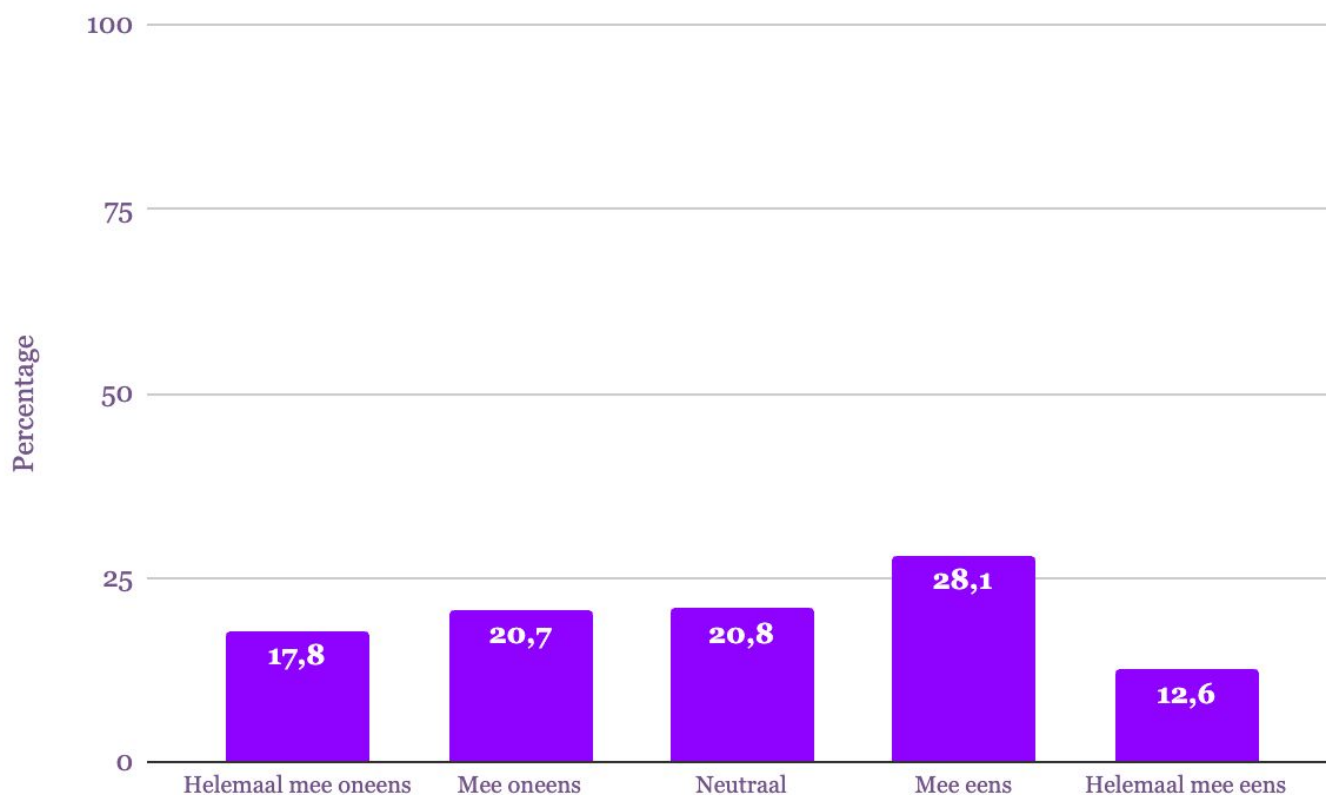
Uitsplitsing op basis van wel/niet zelf opgelicht.



Interpretatie

De groep respondenten die zelf **niet** is opgelicht, laat een aanzienlijk hoger gemiddelde zien bij deze stelling. Dit betekent dat deze groep het vaker eens is met deze stelling en dus vaker denkt dat de kans klein is dat hij/zij/hen slachtoffer zal worden van online oplichting. Het lijkt er dus op dat slachtofferschap van online oplichting ertoe leidt dat je beter inziet dat die kans bestaat.

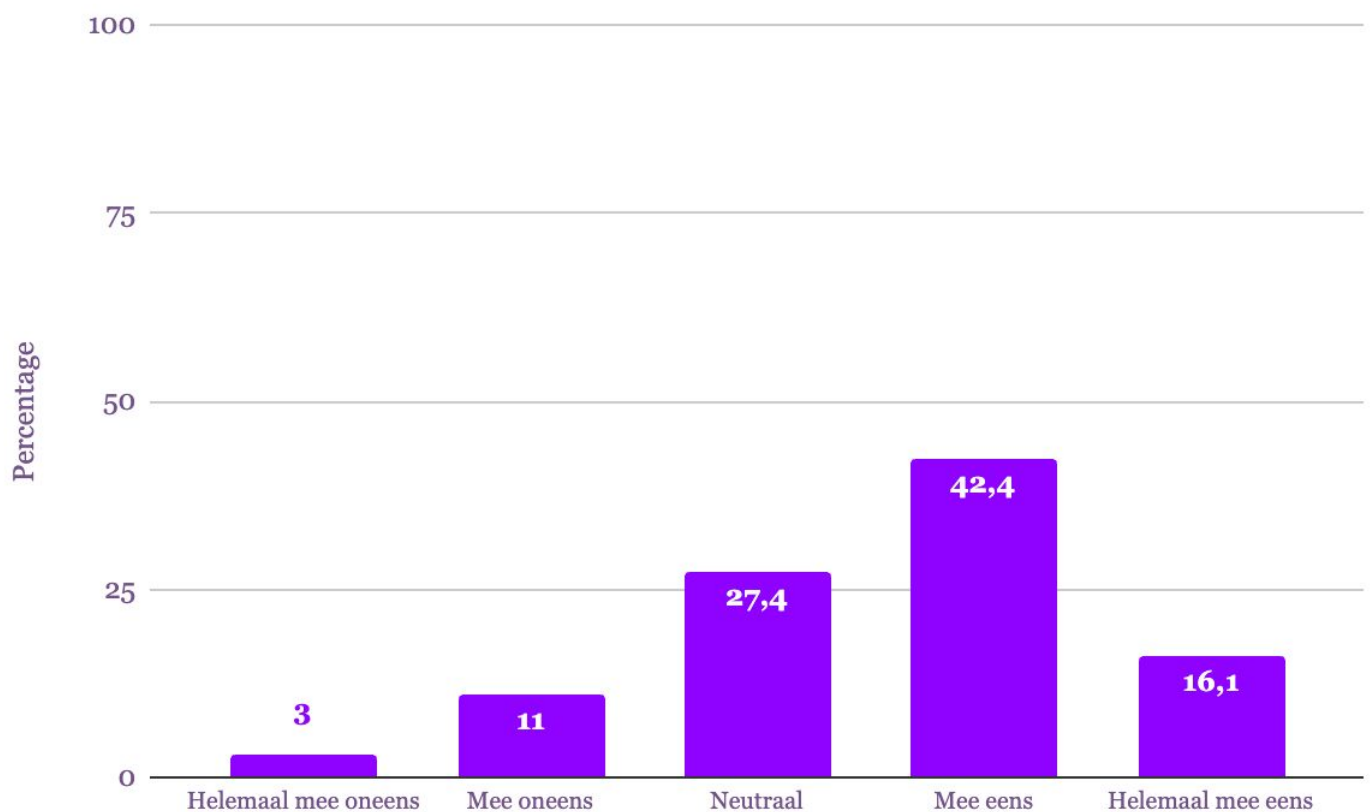
Als ik online opgelicht zou worden, zou ik me daarvoor schamen.



Interpretatie

Een vrij grote groep van ruim 40% geeft aan dat zij zich zouden schamen als ze slachtoffer zijn geworden van online oplichting. Ook bijna 40% is het hier juist niet mee eens en zou zich niet schamen.

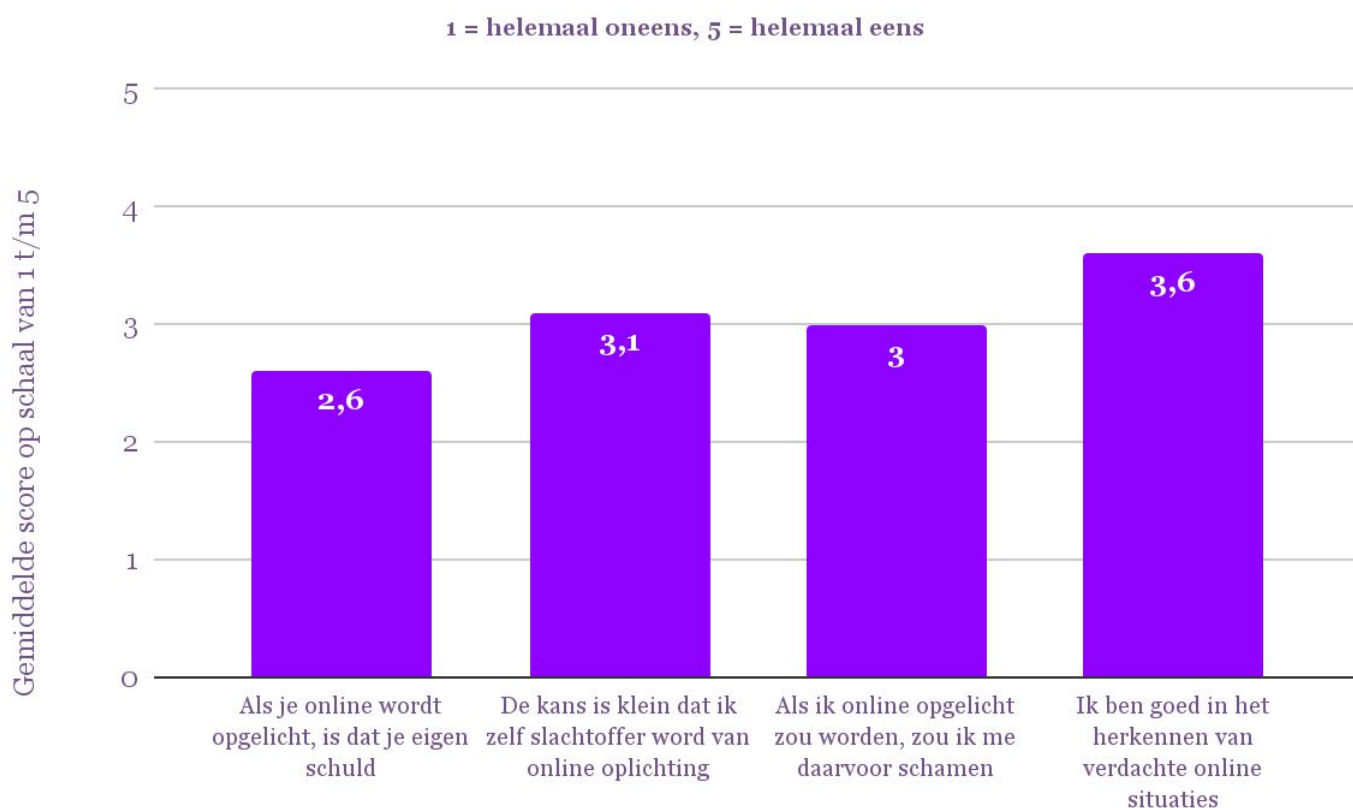
Ik ben goed in het herkennen van verdachte online situaties.



Interpretatie

Bijna 60% van de respondenten vindt zichzelf goed in het herkennen van verdachte online situaties en nog eens 27,4% staat hier neutraal in.

Gemiddelde scores per stelling



Interpretatie

Als we kijken naar de gemiddelde score van respondenten op deze stellingen, zien we dat de respondenten de kans dat ze slachtoffer worden niet zo groot achten en áls het toch gebeurt, is er een aanzienlijke groep die zich hiervoor zou schamen. De respondenten vinden zichzelf overigens erg goed in het inschatten van online verdachte situaties.

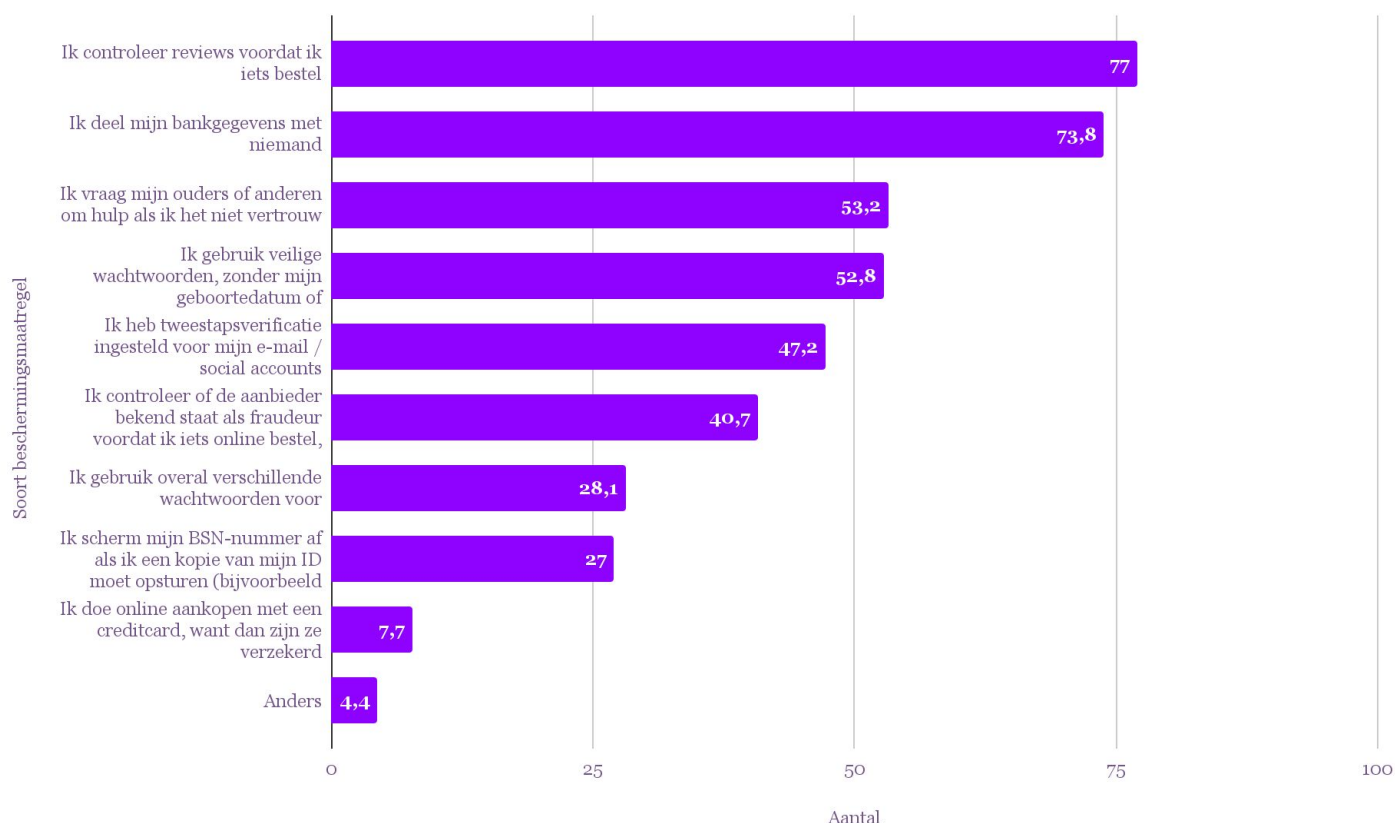
Tegelijkertijd vinden de meeste scholieren toch niet dat slachtoffer worden van online oplichting je eigen schuld is. Ze lijken dus strenger voor zichzelf te zijn dan voor anderen.

Resultaten

Online oplichting voorkomen.

Online oplichting voorkomen

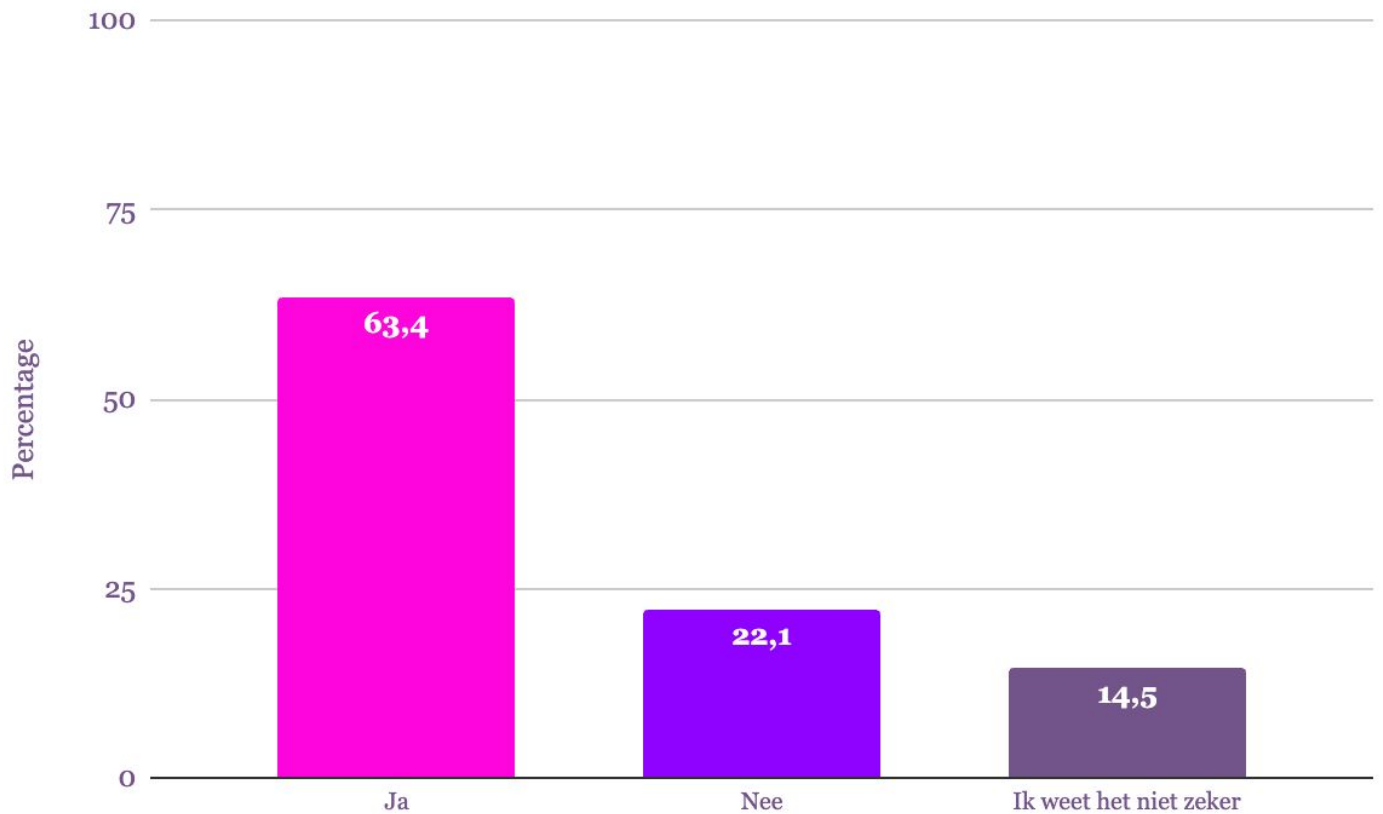
Wat doe je zelf om te voorkomen dat je wordt opgelicht?



Interpretatie

Een aantal maatregelen zijn goed ingeburgerd bij de ondervraagde respondenten. Het gaat om het controleren van reviews (77% doet dit) en het niet delen van bankgegevens (73,8%). Daarnaast zijn er een aantal maatregelen die ongeveer de helft van de respondenten toepast: ouders om hulp vragen (53,2%), veilige wachtwoorden gebruiken (52,8%) en tweestapsverificatie instellen (47,2%). Aankopen doen met een creditcard komt bijna niet voor onder de respondenten (7,7%), waarschijnlijk omdat de respondenten veelal minderjarig zijn. Ook maatregelen zoals het gebruik van verschillende wachtwoorden (28,1%) en gebruik van de kopieID app (27%), worden niet vaak toegepast.

Weet je wat tweestapsverificatie (ook wel tweefactorauthenticatie of 2FA genoemd) betekent?



Interpretatie

Ruim 60% van de respondenten weet wat tweestapsverificatie is. Een kleine 40% weet dit niet, of weet het niet zeker.

Leg uit wat het volgens jou inhoudt

Aan alle respondenten is gevraagd om uit te leggen wat tweestapsverificatie volgens hen betekent.

Als we een samenvatting maken van de antwoorden van de 402 respondenten die aangeven dat zij wel weten wat het inhoudt, zien we dat men dit inderdaad goed weet. In deze antwoorden komen veelvuldig de woorden 'wachtwoord' en 'code' terug. Hierdoor weten we dat respondenten tweestapsverificatie linken aan wachtwoorden met een extra beveiligingscode. Een aantal letterlijke quotes uit de antwoorden:

"Een tweede controle na het intypen van je wachtwoord."

"Extra controle wanneer je ergens moet inloggen met een code via sms of app."

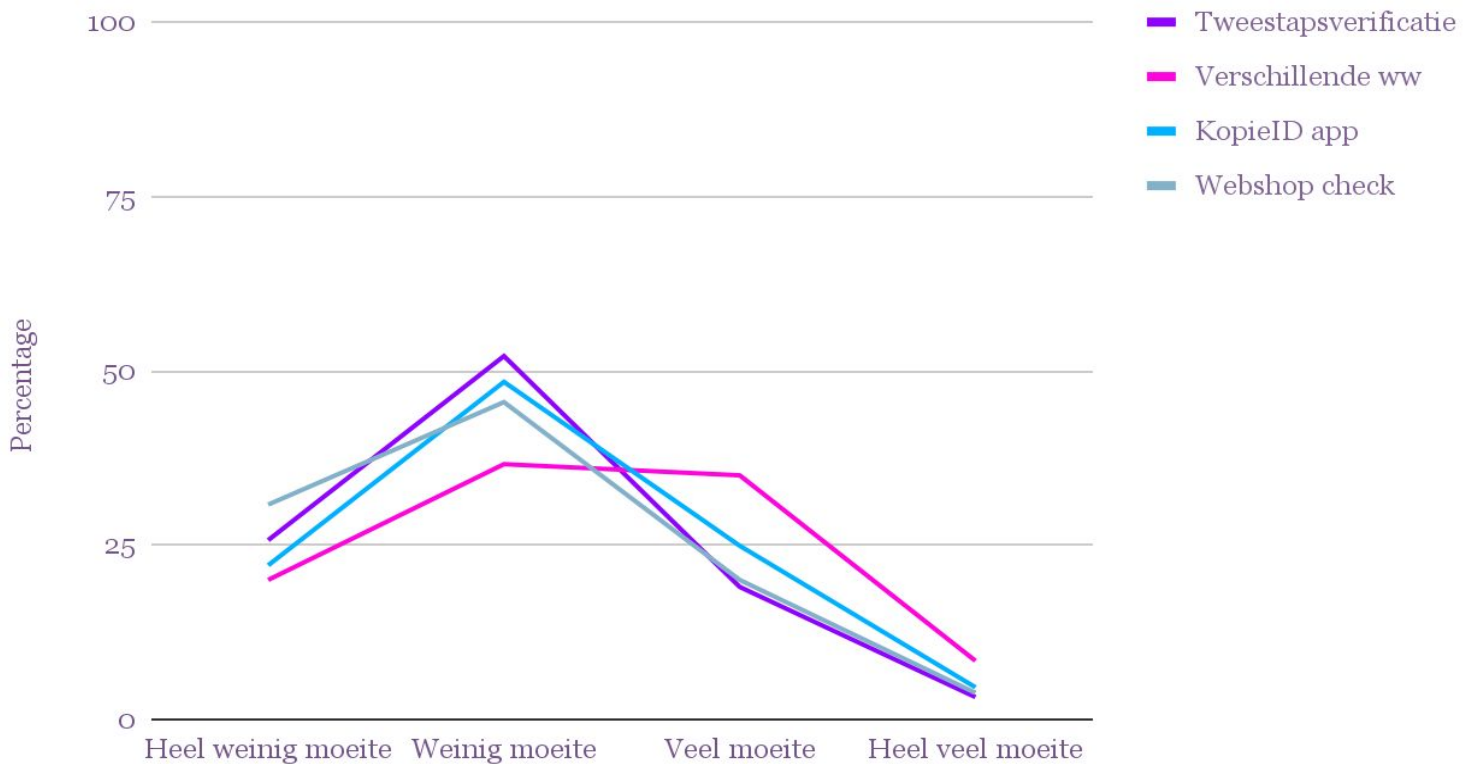
"Dat je naast een wachtwoord je ook verifieert met een code die je via sms of mail krijgt."

Als we de antwoorden analyseren van de 140 mensen die 'nee' hebben geantwoord op de vraag of zij weten wat tweestapsverificatie inhoudt, zien we dat de term voor hen onduidelijk is. De woordcombinaties 'geen idee' en 'weet ik niet' komen vaak terug. Ook zien we een aantal keer voorbij komen dat men wel weet dat het iets met wachtwoorden en beveiliging te maken heeft.

"Volgens mij iets om je account veiliger te maken"

"Dat je twee keer een wachtwoord in moet voeren."

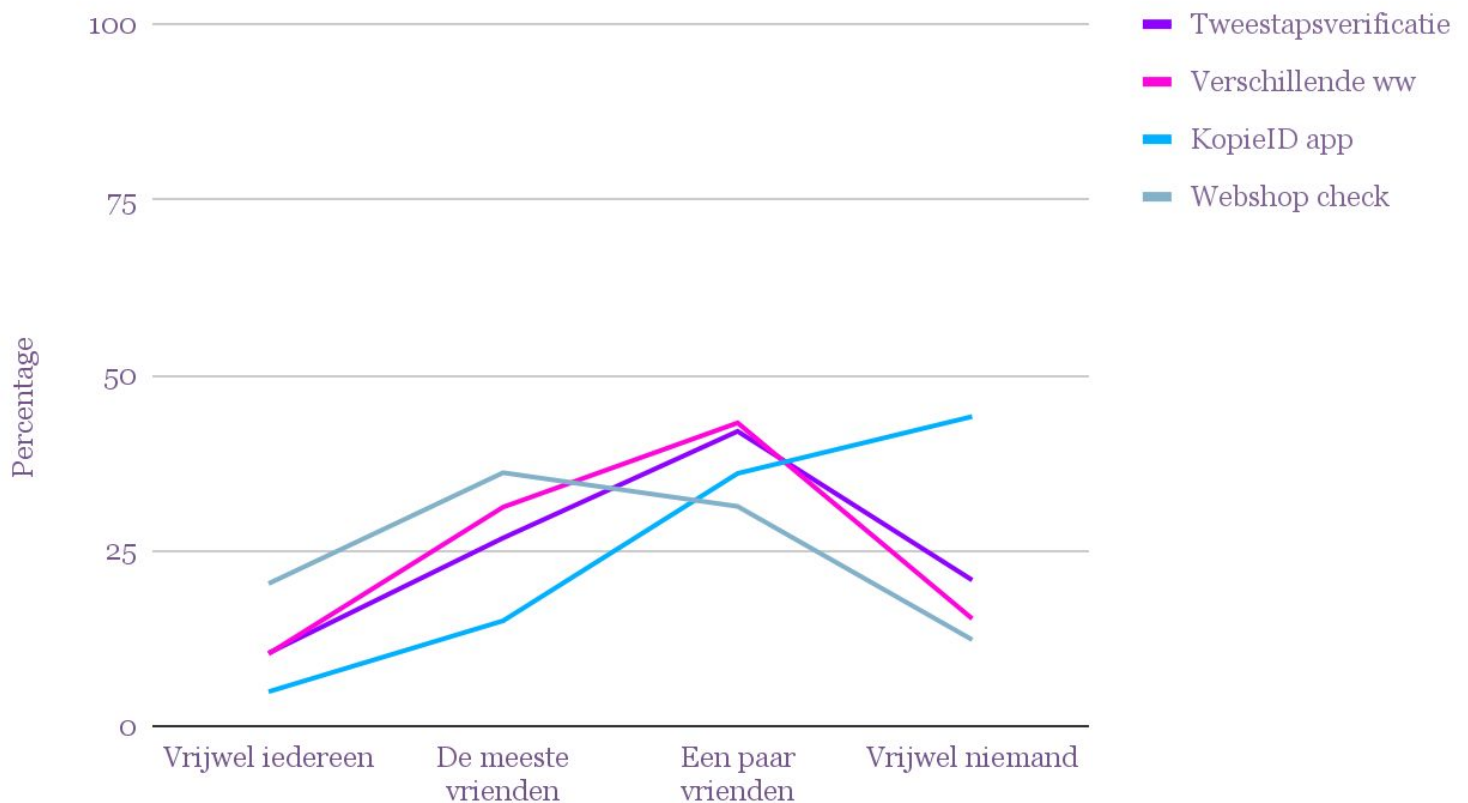
Hoeveel moeite kosten volgens jou de volgende maatregelen?



Interpretatie

Van de voorgestelde maatregelen die je kunt nemen om je te beschermen tegen online oplichting, vinden de respondenten het checken van webshops heel weinig moeite kosten. Het instellen van verschillende wachtwoorden vindt men juist heel veel moeite. Dit komt overeen met het antwoord op een eerdere vraag, waaruit blijkt dat slechts 28,1% verschillende wachtwoorden gebruikt voor alle accounts.

Hoeveel van jouw vrienden zouden de volgende maatregelen nemen?



Interpretatie

Als we de respondenten vragen om een inschatting te maken van welke maatregelen vrienden wel en niet zouden nemen, komt hier ook een duidelijk beeld uit. Een flink deel van de respondenten schat in dat vrijwel niemand van hun vrienden de KopieID app zal gebruiken, ook al geeft men in de vorige vraag aan dat men dat niet heel veel moeite vindt kosten. Het checken van webshops schatten respondenten in als maatregel die wel door veel vrienden opgevolgd zal worden. Dit is ook in lijn met het antwoord op de vorige vraag, waaruit blijkt dat men dit niet veel moeite vindt.

Samenvatting

Samenvatting

Voor dit onderzoek hebben we middelbare scholieren gevraagd naar hun ervaringen met online oplichting, hun houding ten opzichte van online oplichting en de beschermingsmaatregelen die zij nemen.

Ervaringen met online oplichting

Het aantal scholieren dat zegt online te zijn opgelicht, ligt op 36,1%. Dat is een hele lichte stijging ten opzichte van 2017, toen we dezelfde vraag gesteld hebben aan middelbare scholieren (35,4% gaf toen aan online te zijn opgelicht). Jongens antwoorden vaker 'ja' op de vraag of ze zijn opgelicht dan meisjes. Meisjes weten het vaker 'niet zeker'. 47,2% van de scholieren geeft daarnaast aan dat één van hun vrienden online weleens is opgelicht. In 2017 lag ook dit percentage iets lager, op 45,3%.

Scholieren konden zelf aangeven wat hen of hun vrienden is overkomen. Uit de open antwoorden valt op te maken dat de meeste ervaringen neerkomen op een vorm van aankoopfraude: er wordt online een product besteld, dat na betaling niet geleverd wordt (of niet aan de verwachtingen voldoet). Ook als zij hun ervaring moeten indelen bij een van de gegeven vormen van online oplichting, scoort aankoopfraude veruit het hoogst.

Als wordt gevraagd voor welke vorm van online oplichting jongeren het meest kwetsbaar zijn, scoren **aan- en verkoopfraude** opnieuw het hoogst, gevolgd door het **hacken van een e-mail of social media account** en het **klikken op valse links** via e-mail of via een direct bericht (sms, dm, appje).

Houding ten opzichte van online oplichting

Nieuw in dit onderzoek zijn de stellingen om de houding van scholieren ten opzichte van online oplichting te peilen. Uit de antwoorden op de stellingen ontstaat het beeld dat de meeste scholieren het niet je eigen schuld vinden als je slachtoffer wordt van online oplichting. Hierbij is vrijwel geen verschil tussen jongeren die zelf zijn opgelicht en jongeren die niet zijn opgelicht. Als je wordt opgelicht, dan zou ruim 40% van de scholieren zich daar wél voor schamen.

Als we middels een stelling vragen hoe groot scholieren de kans inschatten dat zij zelf slachtoffer worden van online oplichting, zien we dat bijna 40% die kans klein acht. Nog eens 30% staat er neutraal in. Daarnaast denken scholieren dat zij goed zijn in het doorzien van verdachte online situaties: bijna 60% vindt zichzelf hier goed in.

Deze resultaten samen scheppen een beeld van middelbare scholieren die overtuigd zijn van hun capaciteiten om online oplichters door te hebben. Als het dan toch mis gaat, en die kans achten scholieren dus vrij klein, dan is er regelmatig sprake van schaamte. Voor anderen lijken scholieren milder te zijn, want zeggen dat slachtoffer worden van online oplichters je eigen schuld is gaat de meesten toch te ver.

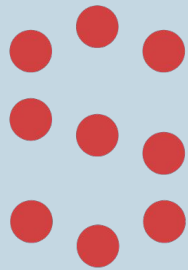
Online oplichting voorkomen

In het vorige deel zagen we dat scholieren de kans dat zij online opgelicht worden vrij laag inschatten. Ze nemen dan naar eigen zeggen ook zeker maatregelen om zich te beschermen tegen online oplichters. Maatregelen die door ongeveer driekwart van de scholieren genomen worden, zijn het **controleren van reviews** en het **niet delen van bankgegevens**. Meer dan de helft van de scholieren **vraagt ook ouders om hulp** als ze ergens over twifelen en gebruikt naar eigen zeggen **veilige wachtwoorden** (zonder geboortedatum of huisdiernamen).

Maatregelen die door veel minder scholieren genomen worden, zijn het gebruik van **verschillende wachtwoorden**, het **afschermen van persoonlijke gegevens** met de KopieID app en het **doen van aankopen met een creditcard**. Dat weinig scholieren de laatste maatregel nemen, is waarschijnlijk te verklaren door het feit dat minderjarigen meestal niet over een creditcard beschikken.

Een belangrijke beschermingsmaatregel is het instellen van tweestapsverificatie op je belangrijke accounts. Deze maatregel eindigt in de middenmoot: 47,2% van de deelnemers zegt dit te doen. Een specifieke vraag over tweestapsverificatie, leert ons dat ruim 60% weet wat dit inhoudt. 22,1% weet het niet en 14,5% weet het niet zeker.

Scholieren geven echter aan dat zij het instellen van tweestapsverificatie niet laten omdat ze het veel moeite vinden. Dat is wél het geval bij het instellen van verschillende wachtwoorden voor al je accounts. Verder valt op dat scholieren verwachten dat vrijwel niemand van hun vrienden de KopieID-app zal gebruiken.



Stemmingmakers

Bijlagen

–

Vragenlijst

Vragenlijst

Jouw ervaring met online oplichting.

1. Ben jij weleens opgelicht?
 - a. Ja
 - b. Nee
 - c. Ik weet het niet zeker
2. Hoe ben je (volgens jou) opgelicht? En door wie of wat?
[Open vraag]
3. Welke omschrijving van oplichting past het best bij jouw ervaring?
 - a. Aankoopfraude webshop (iets gekocht bij een webshop, dat nooit bezorgd is)
 - b. Aankoopfraude tweedehands (iets gekocht bij Marktplaats of Vinted dat nooit bezorgd is)
 - c. Verkoopfraude (je verkoopt iets online en verstuurt het, maar je ontvangt nooit de betaling)
 - d. Op een valse link geklikt via e-mail
 - e. Op een valse link geklikt via Whatsapp, DM of sms
 - f. E-mailadres of social media account gehackt
 - g. Identiteitsfraude (iemand maakt misbruik van jouw persoonsgegevens)
 - h. Fraude betalingsverkeer (je bankrekening beschikbaar stellen voor een paar transacties, tegen een vergoeding)
 - i. Oplichting via nepaccounts of gehackte account van vrienden (geld overmaken naar onbekend persoon)
 - j. Kamerverhuurfraude (voorschot betaald voor kamer die niet bestaat)
 - k. Beleggingsfraude (geld geïnvesteerd in crypto of beleggingen en kwijtgeraakt)
 - l. Lootbox of in-game fraude (aankopen gedaan in een game en die nooit ontvangen)
 - m. Helpdeskfraude of bankfraude (telefonisch benaderd worden door mensen die zich voordoen als een medewerker van een bedrijf of bank)
 - n. Anders, namelijk
4. Is één van je vrienden weleens opgelicht?
 - a. Ja
 - b. Nee
5. Hoe was hij/zij opgelicht? En door wie of wat?
[Open vraag]

6. Van welke vormen van oplichting worden jongeren het makkelijkst slachtoffer, denk jij?
- a. Aankoopfraude webshop (iets gekocht bij een webshop, dat nooit bezorgd is)
 - b. Aankoopfraude tweedehands (iets gekocht bij Marktplaats of Vinted dat nooit bezorgd is)
 - c. Verkoopfraude (je verkoopt iets online en verstuurt het, maar je ontvangt nooit de betaling)
 - d. Op een valse link geklikt via e-mail
 - e. Op een valse link geklikt via Whatsapp, DM of sms
 - f. E-mailadres of social media account gehackt
 - g. Identiteitsfraude (iemand maakt misbruik van jouw persoonsgegevens)
 - h. Fraude betalingsverkeer (je bankrekening beschikbaar stellen voor een paar transacties, tegen een vergoeding)
 - i. Oplichting via nepaccounts of gehackte account van vrienden (geld overmaken naar onbekend persoon)
 - j. Kamerverhuurfraude (voorschot betaald voor kamer die niet bestaat)
 - k. Beleggingsfraude (geld geïnvesteerd in crypto of beleggingen en kwijtgeraakt)
 - l. Lootbox of in-game fraude (aankopen gedaan in een game en die nooit ontvangen)
 - m. Helpdeskfraude of bankfraude (telefonisch benaderd worden door mensen die zich voordoen als een medewerker van een bedrijf of bank)
 - n. Anders, namelijk

Jouw houding ten opzicht van online oplichting.

7. Als je wordt opgelicht, is dat je eigen schuld.
Helemaal mee oneens (1) - helemaal mee eens (5)
8. De kans is klein dat ik zelf slachtoffer word van online oplichting.
Helemaal mee oneens (1) - helemaal mee eens (5)
9. Als ik online opgelicht zou worden, zou ik me daarvoor schamen.
Helemaal mee oneens (1) - helemaal mee eens (5)
10. Ik ben goed in het herkennen van verdachte online situaties.
Helemaal mee oneens (1) - helemaal mee eens (5)

Online oplichting voorkomen.

11. Wat doe je zelf om te voorkomen dat je online wordt opgelicht?
 - a. Ik heb tweestapsverificatie ingesteld voor mijn e-mailadres en/of sociale media accounts
 - b. Ik gebruik veilige wachtwoorden, zonder mijn geboortedatum of huisdiernamen
 - c. Ik gebruik overal verschillende wachtwoorden voor
 - d. Ik vraag mijn ouders of anderen om hulp als ik iets niet vertrouw
 - e. Ik deel mijn bankgegevens met niemand
 - f. Ik scherm mijn BSN-nummer af als ik een kopie van mijn ID moet opsturen (bijvoorbeeld met de KopieID app)
 - g. Ik doe online aankopen met een creditcard, want dan zijn ze verzekerd
 - h. Ik controleer reviews voordat ik iets online bestel
 - i. Ik controleer of de aanbieder bekend staat als fraudeur voordat ik iets online bestel, bijvoorbeeld via de site van de politie.
 - j. Anders, namelijk
12. Weet je wat tweestapsverificatie (ook wel tweefactorauthenticatie of 2FA genoemd) betekent?
 - a. Ja
 - b. Nee
 - c. Ik weet het niet zeker
13. Leg uit wat het volgens jou inhoudt.
[Open vraag]
14. Hoeveel moeite kosten volgens jou de volgende maatregelen?
Heel veel moeite (1) - heel weinig moeite (4)
 - a. Tweestapsverificatie instellen op je e-mail en socials
 - b. Verschillende wachtwoorden gebruiken, zonder geb. datum/huisdiernamen
 - c. KopieID app gebruiken voor foto's van je ID/paspoort/rijbewijs
 - d. Webshops controleren voordat je een aankoop doet
15. Hoeveel van jouw vrienden zouden de volgende maatregelen nemen?
Vrijwel niemand (1) - vrijwel iedereen (4)
 - a. Tweestapsverificatie instellen op je e-mail en socials
 - b. Verschillende wachtwoorden gebruiken, zonder geb. datum/huisdiernamen
 - c. KopieID app gebruiken voor foto's van je ID/paspoort/rijbewijs
 - d. Webshops controleren voordat je een aankoop doet

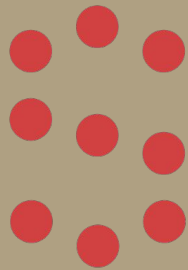
Algemene vragen over jou.

15. Wat is je geslacht?
 - a. Jongen
 - b. Meisje
 - c. Non-binair
 - d. Anders, namelijk

16. Welk niveau doe je?
 - a. Vwo
 - b. Havo
 - c. Vmbo-gt/mavo
 - d. Vmbo-kb
 - e. Vmbo-bb
 - f. Anders, namelijk

17. Hoe oud ben je?
[Open vraag]

18. In welke provincie woon je?
 - a. Limburg
 - b. Noord-Brabant
 - c. Zeeland
 - d. Zuid-Holland
 - e. Gelderland
 - f. Utrecht
 - g. Noord-Holland
 - h. Flevoland
 - i. Overijssel
 - j. Drenthe
 - k. Friesland
 - l. Groningen



Stemmingmakers