

Rapportage
Onderzoek SecuMailer



Datum 14 juli 2020
Kenmerk KP0159

Opdrachtgever:
SecuMailer

Opdrachtnemer:
KiekendiefPerspectief – Drs. Neeske Abrahamse
Schouw 4013
8232 AM Lelystad
Telefoon 0320-228300
E-mail INFO@KIEKENDIEFPERSPECTIEF.NL
Internet WWW.KIEKENDIEFPERSPECTIEF.NL



Inhoudsopgave

1. Inleiding	1
1.1 Achtergrond en aanleiding	1
1.2 Doel	1
1.3 Doelgroep	1
2. Uitkomsten onderzoek SecuMailer	2
2.1 Perceptie en belang van veiligheid bij mailen	2
2.2 Hoe vaak ontvangt men vertrouwelijke info per mail en in welke vorm	3
Bijlage 1. Tot slot, heeft u nog aanvullende op- of aanmerkingen over beveiligd mailen of deze vragenlijst?	6

1. Inleiding

1.1 Achtergrond en aanleiding

SecuMailer is leverancier van veilige e-mail. E-mailen zonder moeite, maar dan wel op de meest veilige manier, dat is al jaren hun missie. Of je nu mail verstuurt of ontvangt, je wilt er zeker van zijn dat er geen letter is gelekt. Dus ontwikkelde SecuMailer een nieuwe technologie om die vervolgens goed te verstoppen – je ziet of merkt er niks van!

SecuMailer wilde graag een onderzoek laten uitvoeren onder e-mail-gebruikers over (veilig) mailen. Onderwerpen die aan bod dienden te komen waren: veiligheid, communicatie (frequentie en vorm) en gebruiksgemak.

1.2 Doel

Het doel van het onderzoek was meervoudig, namelijk inzicht verkrijgen in:

1. De perceptie en het belang van veiligheid bij mailen
2. De communicatie; hoe vaak ontvangt men vertrouwelijke info per mail en in welke vorm
3. Het gebruiksgemak van verschillende vormen van veilig mailen

1.3 Doelgroep

De doelgroep bestond uit e-mail-gebruikers. Een representatieve groep e-mail-gebruikers hebben we bereikt via het FlevoPanel. We hebben hen gevraagd om deel te nemen aan een internetenquête over mailen.

2. Uitkomsten onderzoek SecuMailer

In de periode van 2 t/m 13 juli 2020 zijn middels een elektronische vragenlijst vragen voorgelegd aan e-mail-gebruikers. We hebben een representatieve groep e-mail-gebruikers bereikt via het FlevoPanel (onderzoekspanel van KiekendiefPerspectief). Aan de internetenquête hebben 402 e-mail-gebruikers deelgenomen. Dit is een wetenschappelijk verantwoord aantal.

In dit hoofdstuk wordt ingegaan op de belangrijkste bevindingen van het onderzoek. In paragraaf 2.1 wordt ingegaan op de perceptie en het belang van veiligheid bij mailen. Paragraaf 2.2 behandelt de communicatie, hoe vaak ontvangt men vertrouwelijke info per mail en in welke vorm. Tot slot gaat paragraaf 2.3 in op het gebruiksgemak van verschillende vormen van veilig mailen.

2.1 Perceptie en belang van veiligheid bij mailen

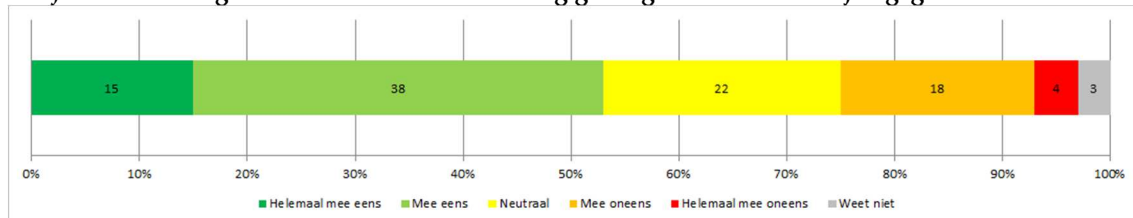
In deze paragraaf gaan we in op de perceptie en het belang van veiligheid bij mailen.

Perceptie veiligheid gewone e-mail bij versturen vertrouwelijke gegevens

We hebben de volgende stelling voorgelegd aan de e-mail-gebruikers en gevraagd in welke mate men het eens of oneens is met de stelling: *Gewone e-mail is niet veilig genoeg om vertrouwelijke gegevens te versturen*. Het resultaat staat in grafiek 1.

Meer dan de helft (53%) van de e-mail-gebruikers is het (helemaal) eens met deze stelling. Verder staat 22% er neutraal in, is eveneens 22% er (helemaal) mee oneens en 3% weet het niet.

Grafiek 1: Stelling: Gewone e-mail is niet veilig genoeg om vertrouwelijke gegevens te versturen



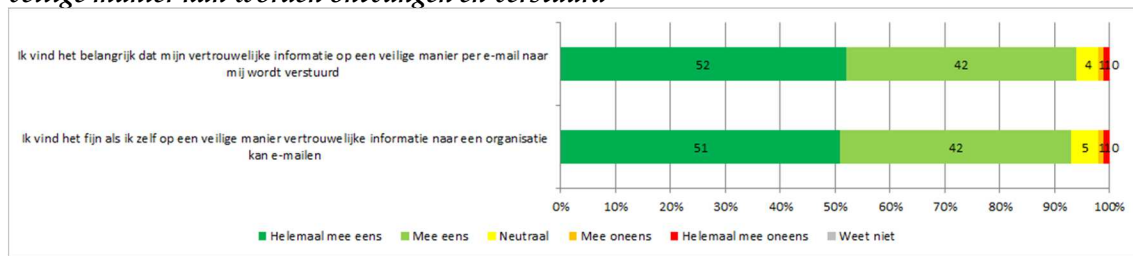
Belang van veiligheid bij mailen

Ook hebben we gevraagd hoe belangrijk men het vindt dat e-mail met vertrouwelijke informatie op een veilige manier kan worden ontvangen en verstuurd, zie grafiek 2.

Het blijkt dat zowel het op een veilige manier ontvangen als het zelf versturen van e-mail met vertrouwelijke informatie belangrijk en fijn wordt ervaren. Bij het ontvangen van mail met vertrouwelijke informatie geeft 94% aan het (helemaal) eens te zijn met de stelling: *Ik vind het belangrijk dat mijn vertrouwelijke informatie op een veilige manier per e-mail naar mij wordt verstuurd*. Slechts 4% staat er neutraal in en 2% geeft aan het er (helemaal) mee oneens te zijn.

Bij het zelf versturen van mail met vertrouwelijke informatie geeft 93% aan het (helemaal) eens te zijn met de stelling: *Ik vind het fijn als ik zelf op een veilige manier vertrouwelijke informatie naar een organisatie kan e-mailen*. Slechts 5% staat er neutraal in en 2% geeft aan het er (helemaal) mee oneens te zijn.

Grafiek 2: Hoe belangrijk vindt men het dat e-mail met vertrouwelijke informatie op een veilige manier kan worden ontvangen en verstuurd



2.2 Hoe vaak ontvangt men vertrouwelijke info per mail en in welke vorm

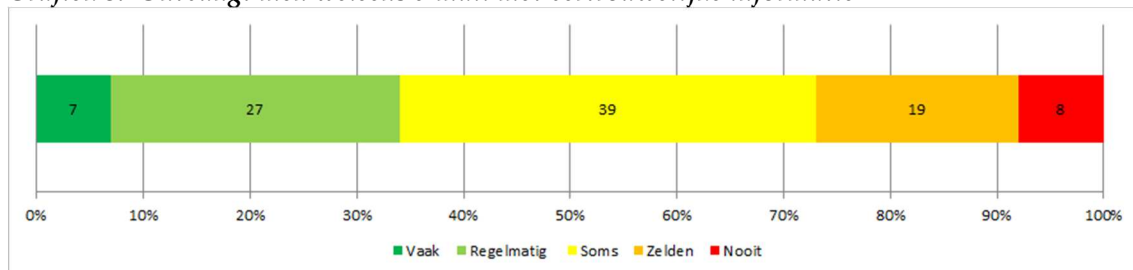
In deze paragraaf gaan we in op de frequentie waarmee men vertrouwelijke informatie per mail ontvangt en in welke vorm.

Frequentie mail met vertrouwelijke informatie

De overheid, de gemeente, banken en andere instanties zoals ziekenhuizen en zorgverzekeraars zijn verplicht om privacygevoelige informatie veilig te versturen. Wij hebben aan de e-mailgebruikers gevraagd hoe vaak men e-mail met vertrouwelijke informatie ontvangt (zie grafiek 3).

Ruim een derde (33%) van de respondenten ontvangt regelmatig of vaak e-mail met vertrouwelijke informatie, 39% soms en 27% zelden of nooit.

Grafiek 3: Ontvangt men weleens e-mail met vertrouwelijke informatie



Ontvangst beveiligde mail en welke vorm

Zoals eerder aangegeven zijn de overheid, de gemeente, banken en andere instanties zoals ziekenhuizen en zorgverzekeraars verplicht om privacygevoelige informatie veilig te versturen. Daarvoor zijn verschillende oplossingsmogelijkheden.

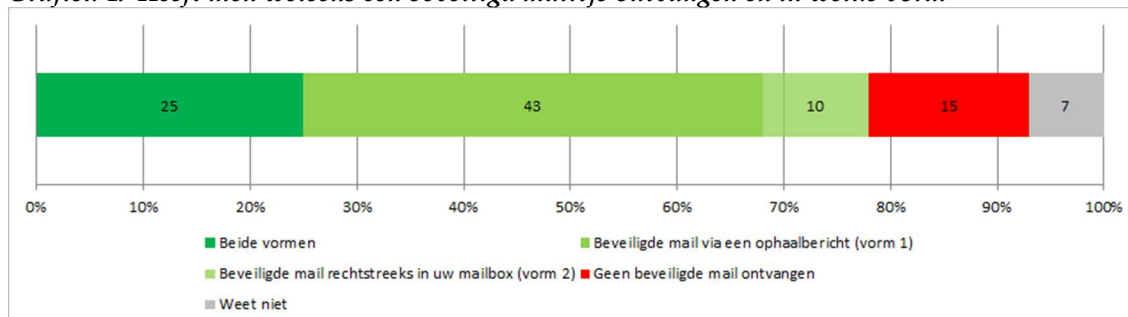
Eén daarvan is met behulp van een ophaalbericht (vorm 1): u ontvangt een e-mail met een link naar een beveiligde omgeving, hier moet u een SMS-code of een toegangscode invoeren om het bericht te kunnen lezen (is het bericht beveiligd met een toegangscode, dan ontvangt u deze apart van de afzender).

Beveiligde e-mail ontvangen kan ook met een andere methode, namelijk op de achtergrond beveiligd, zodat de e-mail op de gewone manier wordt afgeleverd in uw mailbox, zonder dat u extra handelingen hoeft te verrichten (vorm 2).

We hebben gevraagd of men weleens zo'n beveiligd mailtje heeft ontvangen en welke vorm, zie grafiek 4.

Ruim tweederde (68%) heeft weleens een beveiligde mail via een ophaalbericht (vorm 1) ontvangen, ruim eenderde (35%) heeft weleens een beveiligde mail rechtstreeks in de mailbox ontvangen (vorm 2), 15% heeft geen beveiligde mail ontvangen en 7% weet het niet.

Grafiek 4: Heeft men weleens een beveiligd mailtje ontvangen en in welke vorm



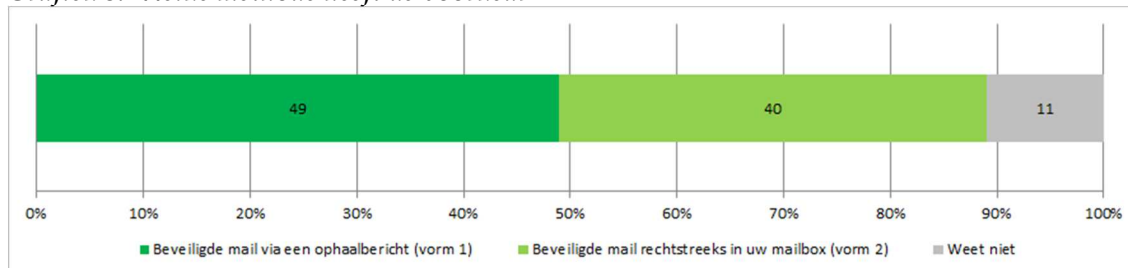
2.3 Gebruiksgemak verschillende vormen van veilig mailen

In deze paragraaf gaan we in op het gebruiksgemak van verschillende vormen van veilig mailen.

Welke methode heeft de voorkeur

Wanneer gevraagd wordt welke methode de voorkeur heeft (zie grafiek 5), geeft bijna de helft (49%) beveiligde mail via een ophaalbericht aan (vorm 1). Circa 40% geeft aan een voorkeur te hebben voor vorm 2. De overige 11% weet het niet.

Grafiek 5: Welke methode heeft de voorkeur



Gebruiksgemak algemeen

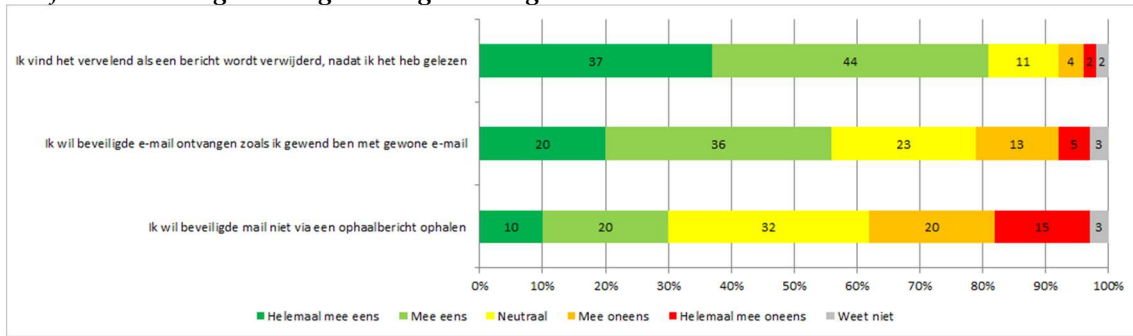
Er zijn een drietal stelling voorgelegd over het gebruiksgemak in het algemeen, zie grafiek 6.

Maar liefst 81% is het (helemaal) eens met de stelling: *Ik vind het vervelend als een bericht wordt verwijderd, nadat ik het heb gelezen.*

Verder geeft ruim de helft (56%) aan het (helemaal) eens te zijn met de stelling: *Ik wil beveiligde e-mail ontvangen zoals ik gewend ben met gewone e-mail.*

En bijna een derde(30%) geeft aan het (helemaal) eens te zijn met de stelling: *Ik wil beveiligde mail niet via een ophaalbericht ophalen.*

Grafiek 6: Stellingen over gebruiksgemak algemeen



Gebruiksgemak beveiligde mail via een ophaalbericht (vorm 1)

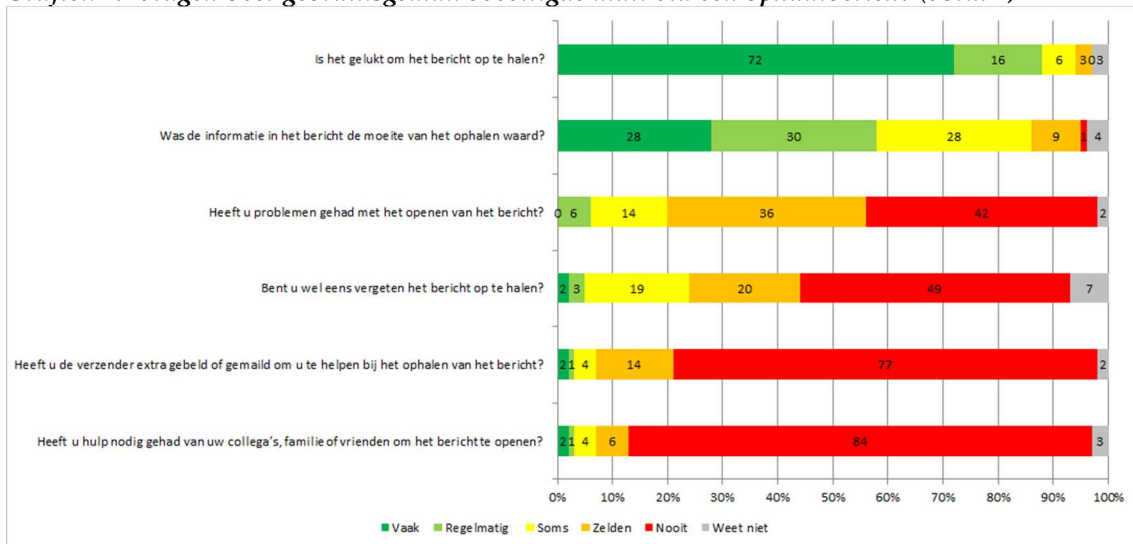
De e-mail-gebruikers die wel eens een ophaalbericht van vorm 1 hebben ontvangen hebben we nog een aantal vragen voorgelegd (zie grafiek 7).

Zo'n 88% geeft aan dat het vaak of regelmatig gelukt is om het bericht op te halen. Verder was de informatie in het bericht vaak of regelmatig (58%) de moeite van het ophalen waard.

Bijna een kwart (24%) geeft aan vaak, regelmatig of soms wel eens vergeet het bericht op te halen. Ongeveer 20% geeft aan vaak, regelmatig of soms problemen te hebben gehad met het openen van het bericht.

Verder geeft 7% aan vaak, regelmatig of soms hulp nodig te hebben gehad van collega's, familie of vrienden om het bericht te openen en heeft eveneens 7% aan vaak, regelmatig of soms de verzender extra gebeld of gemaïld te hebben om te helpen bij het ophalen van het bericht.

Grafiek 7: Vragen over gebruiksgemak beveiligde mail via een ophaalbericht (vorm 1)



Bijlage 1. Tot slot, heeft u nog aanvullende op- of aanmerkingen over beveiligd mailen of deze vragenlijst?

- Als een beveiligd bericht via 'gewone' e-mail komt, hoe weet ik dan dat het beveiligd is? Daarom de 2e keer 'weet niet' ingevuld. Ik vind al die extra stappen wel vervelend, zeker als het gaat om een bericht waarin alleen maar staat dat ik een afspraak kan maken bij een zorgverlener of zoiets
- als ik alleen ben (vooral in corona tijd) durf ik vaak niet van alles te installeren, wacht op steun familie.
- Als ik een certificaat op mijn mail zet moet de andere partij dat ook doen. blijft lastig.
- Banken sturen geen vertrouwelijke informatie per mail, maar doen dat altijd per (ouderwetse) post. E-mail die ik van banken ontvang waarin vertrouwelijke informatie staat of gevraagd wordt, vertrouw ik niet en verdwijnt dan ook direct in de prullenbak.
- Dubbele zekerheid en controle belangrijk
- Er zijn mensen die geen mobiel hebben dus dat geneuzel met een SMS gaat voor hun helemaal niet op. Ook zijn er mensen die sowieso geen mail willen ontvangen van instanties. Ik heb een brievenbus!
- Fijn dat u de u-vorm hebt gehanteerd.
- Ga zo door
- Gewoon via DigiD en dan nog met een sms code dan moet het veilig zijn .Voor belangrijke mail .
- Het is van uiterst belang dat degene die de mail verzend bewust is van zijn / haar actie en dient een collega te laten controleren, gelijk een apotheek, opdat niet een onjuist mailadres wordt gebruikt.
- Het is zeer omslachtig en vaak betreft het helemaal geen vertrouwelijke informatie. Bv een afspraak bij een arts of iets dergelijks. Gewoon mailen is n zo'n geval makkelijker en effectiever
- het ligt er aan welke organisatie de mail verstuurd
- Het meeste gaat in de berichten box van mijn overheid en als reminder krijg je daar en e-mail van. Dat werkt prima en ik ga ervan uit dat dit goed beveiligd is.
- Het nadeel van mailberichten met een link is dat daar ook heel vaak een valse link achter 'verstopt' kan zitten waardoor de betreffende PC besmet kan worden met malware of erger. Dit vergt dan weer lees-discipline van de ontvanger. En ook vaak is de kennis er niet.
- Het zijn heel veel handelingen om een vaak nietszeggend mailtje binnen te halen. Maar ook omgekeerd is het soms te overdreven met niet-accepteren van zgn. persoonlijke informatie. Mijn moeder is diabeet en stuurde in de controle periodes haar waarden naar de specialist. Vanwege de privacygevoeligheid wordt dit geweigerd. Ze geeft niet haar bankrekening en pincode, maar enkel suikerwaardes. Het lijkt alsof de privacy gevoeligheid wel heel erg ver gaat. Enquêteurs zouden dan ook niet meer mogen vragen om geboortedatum, of ik man/vrouw ben, mijn postcode enz.
- Ik ben 76 jaar en voor mij is het altijd moeilijk om zò n bericht te downloaden
- Ik ben ICT'er
- Ik ben tevreden met de methode zoals het gaat. Vertrouwelijke info ophalen met een code en/of SMS bericht.
- Ik hoop dat het ophalen met smscode blijft. Ik heb een heel simpele telefoon waar geen app op kan. Het zou ook goed zijn te vragen hoe mensen hun bericht willen ontvangen, niet elke oudere kan dit met code, dan is gewone mail met beveiliging een uitkomst. Of gewoon per post, in deze tijd v phishingmails wordt je wantrouwig, vooral bij banken
- Ik krijg liever alles per post.
- Ik vind een link onveilig. Je weet nooit of het bericht echt van dit bedrijf is. Ik ben bang om gehackt te worden.

- Ik vind het heel irritant als ik dmv codes via SMS of een nieuwe mail de mail moet openen. Ik vind het ook onzin dat bijvoorbeeld een factuur van de tandarts of mondhygiënist op deze manier wordt ontvangen. Ik download het, en ga het vervolgens versturen naar mijn zorgverzekeraar, en dat doe ik ook niet beveiligd. Ik vind het alleen belangrijk als er een uitslag van een onderzoek in zou staan, of een behandelplan, of een zorgdossier dat wordt overgedragen naar een andere behandelaar.
- Ik wil de belangrijke mail op zo'n veilig mogelijk manier ontvangen.
- Ik wil helemaal geen belangrijke berichten via de computer krijgen. Via de post vind ik veiliger.
- ligt aan de vraagstelling en organisatie
- Nee ik doe veel schriftelijk niet via mijn mail.
- nee opzich niet maar het is fijner als de mails worden beveiligd en in je mailbox kunnen worden geopend. hier is een taak bij voor windows ..
- Niet mogelijk een goede mening te geven zonder enige duiding over de mate van veiligheid van de genoemde opties. Als meer inspanning van mijn kant veiliger is dan prima. Maakt het niet uit dan de optie met de minste inspanning.
- Ondanks de verzekering dat van alles en nog wat veilig is, is volgens mij alles hackbaar. Ik werk om die reden het liefst met DigiD. Dat zal ook wel gehackt kunnen worden maar dan is in ieder geval een andere instantie verantwoordelijk. Verder beveilig ik mijn systemen zo goed als mogelijk en laat regelmatig nakijken op (verwijderen van) spam. Rare berichten open ik niet, berichten van banken die aangeklikt moeten worden open ik ook niet. Fraude meld ik. Ik ben maar een gewone burger en heb niks te verbergen maar het lijkt mij verschrikkelijk als er informatie van mij op straat komt, of (nog erger) dat iemand anders zich als mij voordoe (identiteitsfraude). Helemaal uitroeien gaat niet maar ik vind het belangrijk om er zelf ze veel mogelijk aan mee te werken dat informatie veilig is.
- Pgp bestaat al jaren, maar helaas zijn er te weinig die het (willen) gebruiken
- Sommige spam lijken op ophaalberichten is een groot nadeel
- Soms weten wij niet hoe dit werkt en lukt het niet.
- Toen ik een uitkering had via het UWV, kreeg ik van Mijn Overheid via de email een melding dat er een nieuw bericht in mijn berichtenbox stond. Die melding was dan van het UWV. Maar in de online omgeving van het UWV kreeg ik datzelfde bericht. Dus dat was dubbel. Bovendien was het toen -ik weet niet of dat nu nog zo is- vrij omslachtig om in de berichtenbox van Mijn Overheid te komen.
- Vertrouwelijke gegevens ontvang ik het liefst per post
- Vertrouwelijke mail via DigiD heeft voorkeur
- verwijzing naar een eigen inlog omgeving van de organisatie heeft het meest mijn voorkeur. Bv: u heeft een bericht in uw "mijn overheid"
- Vroeger was er het "briefgeheim". Dat zou de overheid ook middels een wet kunnen regelen betreffende de email. En daar toezicht op houden. Dat zou een sprong vooruit zijn....
- wat wordt verstaan onder vertrouwelijk; ik vind iets niet zo snel vertrouwelijk; de antwoorden hangen dus sterk samen met hoe iemand 'vertrouwelijk' interpreteert