Orange
Cyberdefense

Hoe Nederlanders hun gegevens online beschermen

Opvattingen, basishygiëne en kansen

Inhoudsopgave

Over dit onderzoek

De resultaten in dit rapport zijn afkomstig van een online enquête die in april 2021 is afgenomen onder Nederlandse volwassenen. Aan het door Panelwizard afgenomen onderzoek namen 1.094 Nederlanders deel van 18 jaar en ouder, wat het onderzoek representatief maakt voor heel Nederland.

Geslacht

Man	532
Vrouw	562

Leeftijd

18-29 jaar	201
30-39 jaar	152
40-49 jaar	168
50-59 jaar	199
60+ jaar	374

Gezinssituatie

Eenpersoonshuishouden	243
Huishouden zonder kinderen	573
Huishouden met kind t/m 12 jaar	202
Huishouden met kind van 13+ jaar	76

Opleidingsniveau

Laag	322
Midden	460
Hoog	312

Arbeidsparticipatie

Fulltime (35+ uur)	349
Parttime (12-34 uur)	236
Niet (0-11 uur)	509

Inleiding

Malafide webshops, fraude via Whatsapp of ransomware aanvallen: je leest er dagelijks over in het nieuws. Cybercriminaliteit is niet meer een virus dat op jouw laptop is beland. Criminelen vallen zeer gericht en geavanceerd individuen aan en plegen met hun gegevens identiteitsfraude. Maar het stopt niet bij individuen. Ook grote, gerenommeerde organisaties zijn steeds vaker het slachtoffer van een cyberaanval. Door de digitalisering van de samenleving kan dit grote gevolgen hebben, als bijvoorbeeld hele productieprocessen stil komen te liggen. Zelfs oppermachten als natiestaten mengen zich in deze cyberoorlog. Dat baart ons grote zorgen.

Bij Orange Cyberdefense zijn wij dag en nacht bezig met het analyseren van-, beschermen tegen-, detecteren van- en reageren op digitale dreigingen om onze klanten te beschermen tegen online criminaliteit. Enerzijds kijken we daarbij naar de criminelen. Zoals wij onze technologie verbeteren, verbeteren zijn hun aanvalstactieken. Daarnaast zien we dat criminelen steeds meer tijd nemen voor een aanval en deze specifiek richten op een persoon of organisatie. Tegelijkertijd zijn het opportunisten, ze kiezen de weg van de minste weerstand. Daarom kijken we ook naar hun potentiële slachtoffers. Want zij moeten het criminelen vooral niet te makkelijk maken. Niet alleen als individu, maar ook zeker niet als toegangspoort tot de organisatie waar ze werken. Organisaties kunnen zichzelf nog zo goed beschermen door middel van de laatste technologieën en hun processen goed op orde hebben, maar de Nederlander, en dus de werknemer, blijft een moeilijk te controleren gatekeeper.

Daarom willen wij weten hoe goed Nederlanders hun digitale gegevens eigenlijk beschermen. Hoe gaan Nederlanders om met hardware, met wachtwoorden en instellingen, hoe gedragen ze zich online? Zijn ze zich bewust van de risico's? Wat is de rol van de organisatie in hun cybersecurity bewustzijn? We hebben het onderzocht en delen onze bevindingen in dit rapport. Er is goed nieuws te melden: Nederlanders kunnen het criminelen een stuk lastiger maken met enkele vrij eenvoudige maatregelen. Maar er zijn ook hardere noten te kraken.

Hoofdstuk 1

Het wachtwoord

Het wachtwoord is één van de bekendste en makkelijkste manieren om gegevens te beschermen. Het is alom bekend hoe je verantwoord met je wachtwoord omgaat: deze mag niet gemakkelijk te raden zijn, moet verschillende typen tekens bevatten en moet frequent gewijzigd worden. Hoe zorgvuldig gaat men in praktijk met het wachtwoord om?

1.1 Bepalen

55%
gebruikt hetzelfde wachtwoord voor meerdere accounts

24%
heeft wachtwoord in 5 jaar niet gewijzigd

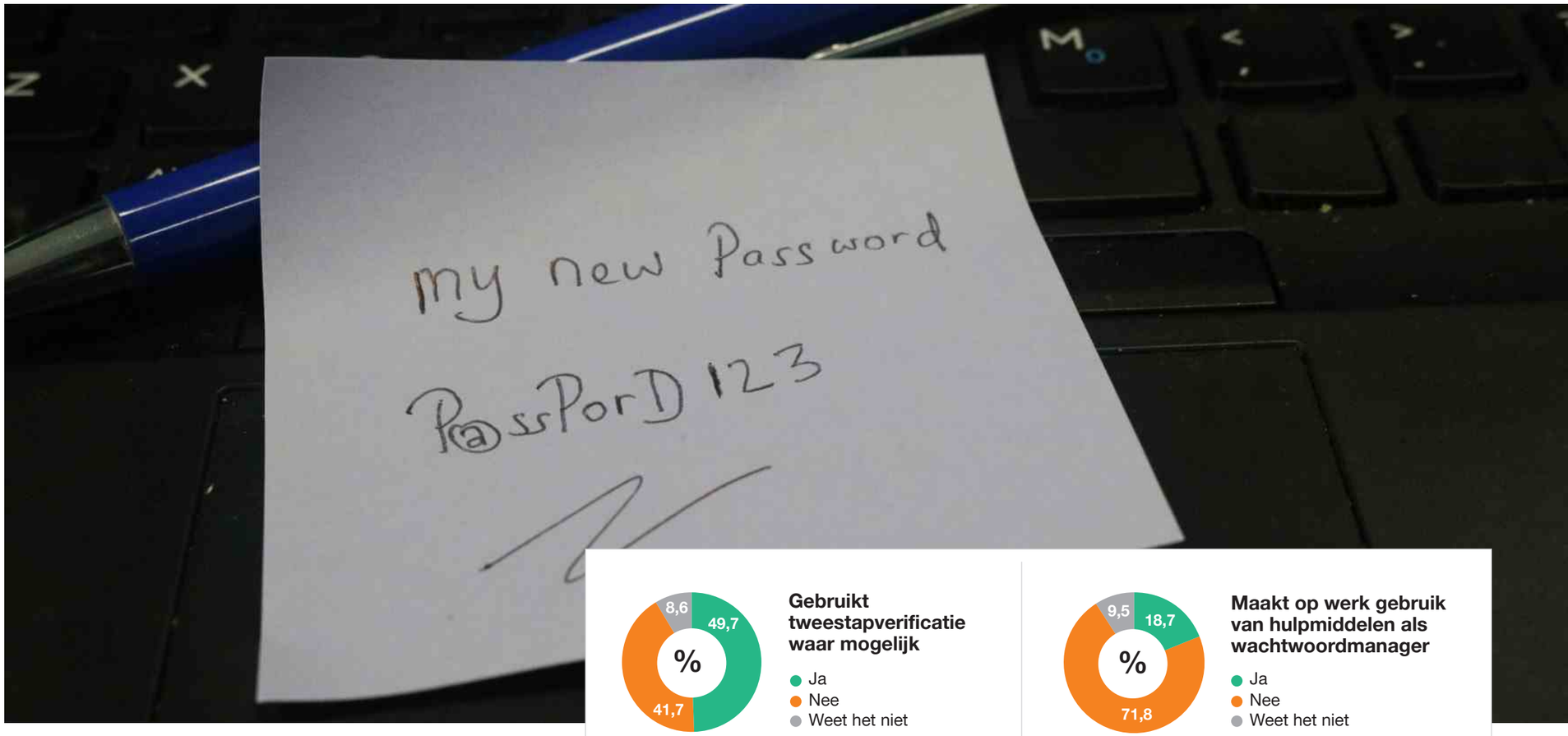
Ruim de helft (55%) van de Nederlanders gebruikt hetzelfde wachtwoord voor meerdere accounts. Een veelgebruikte mogelijkheid is bijvoorbeeld ‘inloggen via Facebook of andere social media’, 47 procent gebruikt die optie waar mogelijk. Waarmee ze gemak boven veiligheid stellen. Ook gebruikt een kwart van de respondenten (27%) hetzelfde wachtwoord zowel voor privé- als voor zakelijke doeleinden. En 17 procent heeft zijn wachtwoord weleens gedeeld met bekenden. Dit is allemaal verre van het geschetste ideaal. Gelukkig begrijpen acht op de tien mensen (80%) uitstekend waarom wachtwoorden aan specifieke eisen moeten voldoen. En de helft (50%) gebruikt tweestapverificatie waar mogelijk. Dat zijn hoopgevender bevindingen.

“Wanneer je hetzelfde wachtwoord voor meerdere toepassingen gebruikt en er bij één ervan je wachtwoord uitlekt, is er vrij toegang tot alle andere toepassingen. Daarom kun je beter voor elke toepassing een uniek wachtwoord gebruiken, die niet makkelijk te raden is en die je met niemand deelt.”

1.2 Wijzigen

Een goede manier om te garanderen dat het wachtwoord frequent wordt vernieuwd, is het verplicht stellen. Bij 21 procent van de Nederlanders vereist de app of het programma waar ze mee werken dat het wachtwoord maandelijks wordt vernieuwd, bij de ruime meerderheid (75%) is dat echter niet het geval. Zo kan het komen dat een kwart (24%) van de respondenten zijn meest gebruikte wachtwoord al vijf jaar niet heeft gewijzigd. Mocht er een melding komen dat een onbevoegd persoon toegang had tot het account, wijzigt negen op de tien (88%) Nederlanders direct zijn wachtwoord. Een kans voor open doel, die toch nog zeven procent onbenut laat.

“Gebruik je voor elke toepassing een uniek wachtwoord en wordt deze bovendien aangemerkt als sterk, dan is er geen reden om je wachtwoord te vernieuwen. Maar wanneer je wachtwoord is gecompromitteerd, bijvoorbeeld bij een datalek, ligt de toegang tot je account op straat of zelfs op de zwarte markt. Dan kun je maar beter zo snel mogelijk een nieuw wachtwoord instellen. Het slot van je voordeur laat je ook vervangen wanneer er is ingebroken of wanneer je de sleutel verloren bent.”



Gebruikt tweestapverificatie waar mogelijk

- Ja
- Nee
- Weet het niet

Maakt op werk gebruik van hulpmiddelen als wachtwoordmanager

- Ja
- Nee
- Weet het niet

1.3 Bewaren

Er zijn veel plekken waar wachtwoorden benodigd zijn, er worden steeds complexere eisen aan gesteld en ze moeten frequent veranderen. Dat kunnen mensen niet in hun hoofd prenten, zoals met een pincode wel kan. Dus worden wachtwoorden op een andere manier onthouden.

Bijna de helft (48%) van de Nederlanders noteert wachtwoorden op een briefje, 27% bewaart ze op de telefoon en 18% in een map op de computer. Een veiliger manier is om hulpmiddelen te gebruiken zoals een wachtwoordmanager. Ruim een derde (35%) van de Nederlanders maakt hier gebruik van. Zakelijk is dit gebruik nog wat minder doorgedrongen, twee op de tien (19%) Nederlanders gebruikt een wachtwoordmanager op het werk. In 85 procent van deze gevallen mag de wachtwoordmanager uitsluitend voor werk worden gebruikt, niet voor privédoeleinden.

In mapje op computer	*18%*
Op telefoon	*27%*
Op papier	*48%*
Wachtwoordmanager	*35%*

“Het noteren van een wachtwoord – op een briefje of digitaal – is vergelijkbaar met het neerleggen van de huissleutel onder de deurmat. Criminelen kunnen het makkelijk vinden. Wachtwoorden kun je beter onthouden met een wachtwoordmanager, een veilige toepassing waar criminelen niet in kunnen. Met zo’n wachtwoordmanager kun je ook sterke en complexere wachtwoorden gebruiken, die nog lastiger zijn te kraken. Ook kun je uitstekend een wachtwoordmanager gebruiken voor privé- en daarnaast één voor zakelijke doeleinden.”

Hoofdstuk 2

Apparatuur en instellingen

Naast het wachtwoord speelt ook de omgang met hardware een belangrijke rol bij de bescherming van gegevens. Zo kun je met een paar relatief eenvoudige instellingen het kwaadwillenden aanzienlijk lastiger maken.

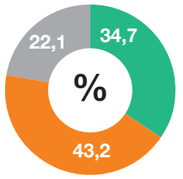
2.1 Privé versus werk

Ruim een derde (35%) van de Nederlanders gebruikt privéapparatuur ook weleens voor zakelijke doeleinden. Andersom is dat ook het geval: 33 procent gebruikt zakelijke apparatuur weleens voor privédoeleinden. Dit gemixte gebruik van hardware vergroot het risico. Zo kan een hack op privé-apparatuur mogelijk toegang bieden aan de zakelijke omgeving. Ook zijn extra security-maatregelen op zakelijke hardware – bijvoorbeeld voor phishing – niet van kracht wanneer deze privé wordt gebruikt.

2.2 Instellingen

61%
logt automatisch in bij openen e-mailprogramma

Door de juiste instelling van je hardware en programma's kun je gegevens beter beschermen. Zo heeft bijna de helft (49%) van de Nederlanders de instelling 'locatie delen' op de telefoon al standaard uit staan. Uitstekend. Bij vier op de tien (41%) is dit echter niet het geval. Dat geldt ook voor andere instellingen, zo hebben ongeveer evenzoveel Nederlanders (40%) bluetooth nog niet standaard uitgeschakeld. Nu is dat vanuit security-oogpunt relatief onschuldig, maar het gaat om het principe: schakel functionaliteit uit wanneer je het niet gebruikt. Dan kunnen anderen er ook niet ongemerkt hun voordeel mee doen.



Gebruikt privé apparatuur ook weleens voor werk

- Ja
- Nee
- Weet het niet

Een andere instelling die het leven weliswaar makkelijker, maar zeker niet veiliger maakt, is automatisch inloggen. Dan hoeft de gebruiker geen inlognaam en wachtwoord in te voeren, maar doet de apparatuur dat op eigen houtje. Bijna twee derde (61%) van de Nederlanders logt automatisch in wanneer ze het e-mailprogramma opstarten. 44 procent heeft de webbrowser zo ingesteld dat er automatisch wordt ingelogd zodra er een website wordt geopend waar ze een account hebben. Bij internetbankieren zijn Nederlanders meer bedachtzaam, negen op de tien (90%) logt nooit automatisch in. Toch doet nog steeds 8 procent dat wel. Allemaal keuzes die best nog eens overdacht mogen worden.

"Automatisch inloggen is gemakkelijk. Maar wanneer je even van je werkplek weg bent en je systeem niet meteen gelockt is, heeft elke voorbijganger direct toegang tot al je toepassingen."

2.3 WiFi

69%
gaat zonder nadenken akkoord met gebruik WiFi-voorwaarden

Veel mensen maken gebruik van een draadloos netwerk. Dat is prettig werken, maar doordat gegevens door de lucht worden verstuurd, is data ook kwetsbaarder. Thuis heeft vrijwel iedereen (91%) zijn WiFi-netwerk beveiligd met een wachtwoord. In meer dan de helft van de gevallen (52%) is dit wachtwoord sinds de installatie echter nog nooit gewijzigd. Het door de fabrikant meegeleverde wachtwoord van de router is nog steeds van kracht. Dat is onverstandig, de fabrikant en mogelijk ook de installateur kennen het. Door derde gecreëerde wachtwoorden zijn bekend bij derden, daarom dien je deze altijd te wijzigen.

Bijna twee derde (62%) van de Nederlanders maakt weleens gebruik van een openbaar WiFi-netwerk. Ruim een kwart (27%) doet dat met een zakelijke laptop of telefoon. Bovendien gaat twee derde (69%) blind akkoord met de gebruiksvoorwaarden van het betreffende WiFi-netwerk. Het is hen dus onbekend hoe het netwerk is beveiligd en wie er eventueel kunnen meekijken.

"Openbare WiFi-netwerken zijn vandaag veiliger dan voorheen, je wordt niet zomaar meer afgeluisterd. Maar de ene WiFi is de andere niet en het is nog steeds onverstandig om zomaar een openbaar netwerk te gebruiken voor zaken. Pas als je zeker weet – soms staat dat in de gebruiksvoorwaarden – dat er met VPN een beveiligde internetverbinding wordt opgebouwd, kun je het zakelijk gebruiken."

Hoofdstuk 3

Houding en gedrag

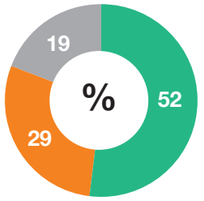
Naast wachtwoorden en instellingen van apparatuur zijn we nu bij een complexer onderwerp beland dat bijdraagt aan de bescherming van gegevens: persoonlijk gedrag. Zo heeft bijna de helft (49%) van de Nederlanders weleens een kopie van zijn of haar legitimatiebewijs via e-mail verstuurd. Zoiets gebeurt soms zonder nadenken, maar vaak is gedrag ook gebaseerd op opvattingen. Dit hoofdstuk biedt een inkijkje in dit gedrag en de achterliggende opvattingen.

3.1 Voorwaarden en cookies

Heb je de privacy-voorwaarden van websites en apps weleens gelezen? Veel Nederlanders niet. Negen op de tien Nederlanders (89%) vinden de voorwaarden te lang, twee derde (65%) vindt ze te complex. Een gevolg is dat driekwart van de Nederlanders (74%) de privacy-voorwaarden van websites en apps blindelings accepteert. Ook cookies op websites worden volop geaccepteerd, zeventig procent staat deze toe.

“Heel risicovol is dit ook weer niet, maar deze mensen hebben daarmee geen idee hoe er met hun gegevens wordt omgesprongen. Bedenk dat een maker ook aan gratis apps geld wil verdienen en dus worden gebruikersdata over online gedrag en persoonsgegevens veelvuldig commercieel verhandeld, bijvoorbeeld aan aanbieders van advertenties. De overheid probeert overigens meer grip te krijgen op deze gebruiksvoorwaarden, die nu vaak bewust onduidelijk geformuleerd en onnodig lang zijn.”

3.2 Opvattingen

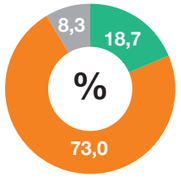


Eigen persoonsgegevens en online gedrag zijn waardevol voor derden

- Ja
- Nee
- Weet het niet

De helft van de Nederlanders (48%) twijfelt of zijn eigen persoonsgegevens en online gedrag waardevol zijn voor bedrijven, of is ervan overtuigd dat dit geen waarde heeft. Negentien procent zegt zelfs dat iedereen zijn data mag hebben, omdat ze toch niets te verbergen hebben. En van acht procent mogen bedrijven met hun persoonlijke gegevens doen wat ze willen. Het interesseert hen niet. Dit betreft weliswaar niet de meerderheid, maar het is toch een behoorlijke groep Nederlanders die zich deze achteloze houding heeft toegemeten. Dat is des te zorgwekkender doordat het gebaseerd lijkt op een misplaatst vertrouwen. Zo denkt 21 procent van de Nederlanders dat alle bedrijven netjes met zijn gegevens zullen omgaan. Je kunt je afvragen of dat vertrouwen terecht is.

“Veel bedrijven hebben inderdaad geen kwaad in de zin en die paar irritante advertenties nemen veel mensen voor lief. Dat resulteert in deze achteloze houding. Maar pas op voor identiteitsfraude. Het risico daarop is weliswaar klein, maar wanneer het je overkomt is de impact enorm. Dat kan bijvoorbeeld gaan om financiële fraude of je kunt afgeperst worden als je medische gegevens op straat liggen. Dat kun je beter niet te los opvatten.”



Ik heb niets te verbergen, iedereen mag mijn data hebben

- Ja
- Nee
- Weet het niet

Zijn Nederlanders dan niet kritisch? Toch wel, en dan vooral op de overheid. De helft van alle Nederlanders (49%) gelooft niet dat zijn persoonsgegevens bij de overheid veilig zijn. Nog eens een kwart (23%) twijfelt daaraan. Ook op het bedrijfsleven is kritiek. Zes op de tien (58%) Nederlanders vinden dat bedrijven klantgegevens teveel aanwenden voor commercieel gewin. Dat mag wel wat minder.

3.3 Techreuzen

Er zijn een handvol bedrijven – Google, Amazon, Facebook en Apple – die onze digitale wereld overheersen. Acht op de tien Nederlanders (81%) maakt zich er druk om dat deze vier techreuzen over zoveel data beschikken. Driekwart (74%) vindt dat we te afhankelijk van hen zijn geworden. Zo voelt ruim de helft (53%) van de Nederlanders zich verplicht om data met de techreuzen te delen, wil je een beetje ‘normaal’ digitaal leven hebben.

Willens en wetens stuurt bijna de helft van de Nederlanders (46%) weleens privégegevens via e-mail of Whatsapp – eigendom van Facebook – naar anderen. Maar over de beveiliging daarvan bestaan grote twijfels. Slechts 16% denkt dat Whatsapp zo goed is beveiligd dat uitsluitend de ontvanger de inhoud kan lezen. Alle anderen twijfelen daaraan of zijn ervan overtuigd dat onbevoegden kunnen meelezen. Dat brengt een bescheiden tegenbeweging op gang:

5% maakt geen gebruik (meer) van Whatsapp, omdat ze zich niet comfortabel voelt met de nieuwe privacy-voorwaarden

22% heeft bewust geen Facebook-account (meer), omdat het te onduidelijk is wat Facebook met de gegevens doet

15% maakt bewust geen gebruik (meer) van Google Maps, omdat ze niet wil dat verplaatsingen worden bijgehouden

Hoofdstuk 4
Criminaliteit

Is het wel nodig om zo ingewikkeld te doen om onze gegevens te beschermen? Dat is en blijft natuurlijk een individuele keuze. Maar veel Nederlanders hebben onprettige ervaringen opgedaan en zijn slachtoffer geworden van online criminaliteit.

4.1 Slachtoffer van crime

gehackt	*15%*
phishing (mail/sms)	*6%*
Whatsapp-fraude	*3%*
frauduleuze webshop	*27%*
ransomware	*13%*

Ruim een kwart van de Nederlanders (27%) heeft weleens iets besteld bij een frauduleuze webshop, waarna ze konden fluiten naar het product én naar hun geld. Fraude via Whatsapp komt veel beperkter voor, slechts drie procent van de Nederlanders zegt daar ooit slachtoffer van te zijn geweest. Het is dan ook een relatief nieuw verschijnsel. Phishing bestaat al langer, maar toch zegt slechts een beperkte zes procent van de Nederlanders daar weleens in te zijn getrapt. Ransomware wordt aanzienlijk vaker genoemd, dertien procent van de Nederlanders heeft weleens ransomware op één van zijn apparaten gehad, waarna vier procent daadwerkelijk geld overmaakte naar de gijzelnemer. Vijftien procent van de Nederlanders zegt weleens gehackt te zijn.

“Pas op voor ransomware, dat maakt een enorme opmars. Maar liefst dertien procent van de Nederlanders heeft er al eens mee te maken gekregen. En gezien de kans op lucratief succes met ransomware, zal dat percentage zeker nog toenemen.”

4.2 Hacken

De hacker wordt gevreesd. 42 procent van de Nederlanders is bang dat hij gehackt wordt en dat al zijn gegevens dan op straat komen te liggen. Evenzoveel mensen (44%) vrezen daar niet voor en negen procent kan het niets schelen. Maar iedereen is het erover eens dat je je maar lastig kunt beschermen tegen hackers. Zo denken acht op de tien Nederlanders (81%) dat een goede hacker overal wel kan binnenkomen, ongeacht de beveiliging. Toch is de kennis over de mogelijkheden van hacken beperkt. Op de vraag of een smartphone gehackt kan worden zijn de meningen verdeeld: de helft (49%) denkt van wel, een kwart (23%) is overtuigd van het tegenovergestelde, en de rest heeft geen idee.

De ene groep Nederlanders voelt zich kwetsbaar, want een hacker komt toch overal wel in. Dat klopt, maar met goede beveiliging kun je hem wel ontmoedigen. Een andere groep Nederlanders denkt dat ze niets te verliezen heeft, de zorgwekkende nonchalante houding die we al eerder zagen. Wat vooral opvalt is dat – ondanks dat een hacker tot de verbeelding van velen spreekt – de feitelijke kennis beperkt lijkt. Zie bijvoorbeeld hoe de meningen verdeeld zijn over hoe kraakbaar een smartphone is. Zo zullen veel mensen zich ook niet kunnen voorstellen hoe vervelend het is wanneer een hacker aan de haal gaat met je BSN, medische of financiële gegevens.”

4.3 Identiteitsfraude

Stel, jouw goede vriend staat met een geblokkeerde bankpas in het buitenland en vraagt jou om hulp. Veel mensen zijn dan bereid geld over te maken. Regelmatig blijkt achteraf dat de identiteit van je vriend is ‘geleend’ door een onbekende, die er nu met je geld vandoor is. Dit soort fraude komt steeds vaker voor. Gelukkig blijkt dat driekwart van de Nederlanders (74%) alleen ingaat op een betaalverzoek via mobiel als het nummer in zijn adresboek staat. Dat voelt inderdaad vertrouwd, maar dan nog is alertheid geboden. Want weet je echt zeker dat het niet iemand anders is die zich voordoet als jouw goede vriend?

Twee op de tien Nederlanders (21%) heeft online weleens contact gehad met iemand die zich als iemand anders voordeed. Twee derde (68%) zegt dat dit nog nooit is voorgekomen en twaalf procent zegt heel slim dat ze het niet weten. Want dat is het hele probleem: je weet niet of de identiteit van de ander klopt. Met meer zekerheid kun je iets over jezelf zeggen. En zeven procent van de Nederlanders zegt zich online weleens te hebben voorgedaan als een ander – om wat voor reden dan ook.

“Twijfel je aan iemands ware identiteit? Verifieer de identiteit dan op een andere manier, bijvoorbeeld door de persoon in kwestie te bellen of door te vragen naar informatie die alleen deze persoon kent, bijvoorbeeld de naam van jouw kat. Ook kun je kritisch bekijken of de inhoud van het bericht en de manier van spreken past bij hoe jij die persoon of dat bedrijf kent. Pas extra op wanneer je wordt gevraagd geld over te maken naar een onbekend rekeningnummer. Vraag dan eerst bij de bank na wie de rekeninghouder is, dan weet je zeker met wie je zakendoet.”

4.4 Onzeker

Op het gebied van digitale criminaliteit voelen veel Nederlanders zich kwetsbaar. Meer dan de helft (56%) heeft het afgelopen jaar maatregelen getroffen om zijn gegevens beter te beschermen. Maar hoe moet dat precies? Er is behoefte aan kennis. Een kwart (23%) van de Nederlanders heeft via werk weleens een training gehad om veilig met gegevens om te gaan, maar de ruime meerderheid (72%) heeft nog nooit zo’n training gevolgd. 43 procent van de Nederlanders vindt dan ook dat er onvoldoende voorlichting wordt geboden door overheid en bedrijven.

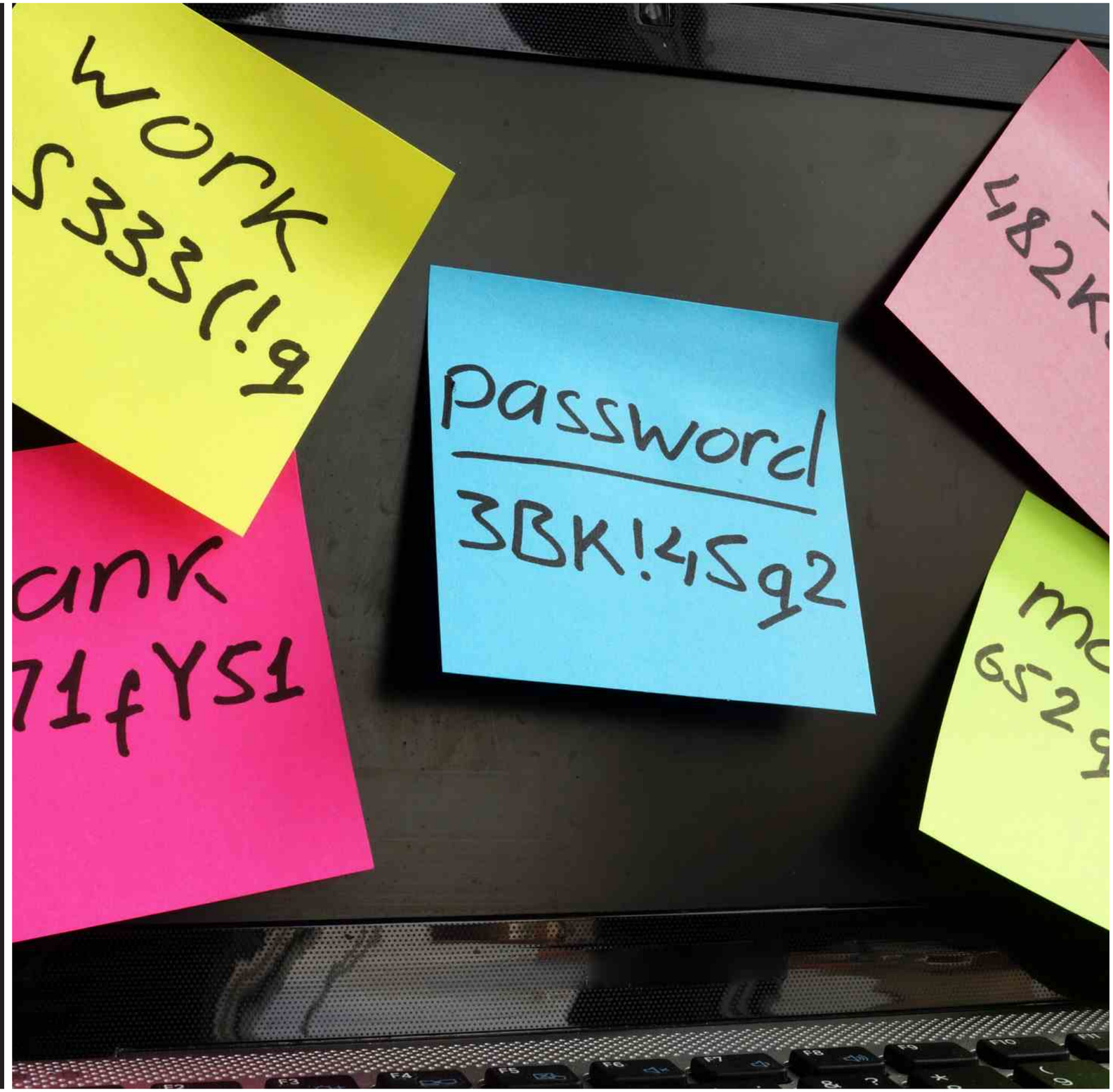
Conclusie: werk aan de winkel

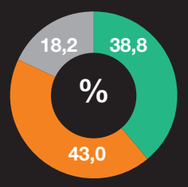
Veel Nederlanders voelen zich online kwetsbaar. Ze hebben het idee dat ze wel ja en amen móeten zeggen tegen techreuzen. En door de lange lappen onbegrijpelijke tekst worden overal maar klakkeloos cookies en privacy-voorwaarden geaccepteerd, zonder dat men eigenlijk weet wat het betekent.

Een groot gevaar dat dreigt en zich ook al volop in de maatschappij nestelt, is een onverschilligheid ten opzichte van security. Er is een grote groep Nederlanders die uit gemakzucht overal dezelfde wachtwoorden gebruikt, deze zelden aanpast en constant automatisch inlogt. Het lijkt hen niet uit te maken hoe bedrijven met hun persoonsgegevens omgaan. Velen steken hun kop bewust in het zand, anderen lijken zich niet bewust van het gevaar. Linksom of rechtsom: het ontbreekt aan een gezonde kritische houding.

Tegelijk vallen veel Nederlanders ten prooi aan digitale criminaliteit. Ze worden slachtoffer van frauduleuze webshops, ransomware of hacks. Er is dan ook een grote groep Nederlanders die de urgentie voelt om haar security te verbeteren. Naar eigen inzicht ondernemen deze Nederlanders daartoe ook acties, maar ze voelen zich daarbij onzeker over welke stappen ze kunnen nemen.

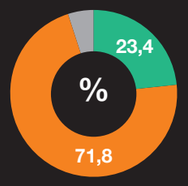
Dit rapport laat zien dat er veel laagdrempelige kansen klaarliggen om benut te worden. Zo kunnen Nederlanders zich acuut beter beschermen door alleen al zorgvuldiger om te gaan met wachtwoorden. Ook in hard- en software hoeven simpelweg enkele instellingen aan- en uitgevinkt te worden, waarna gegevens aanzienlijk beter beschermd zijn. Maar dan moeten gebruikers wel begrijpen waartoe die instellingen dienen en hoe je ze kunt in- of uitschakelen. Aan die kennis ontbreekt het nu. Hier ligt een enorm potentieel voor eenvoudige voorlichting.





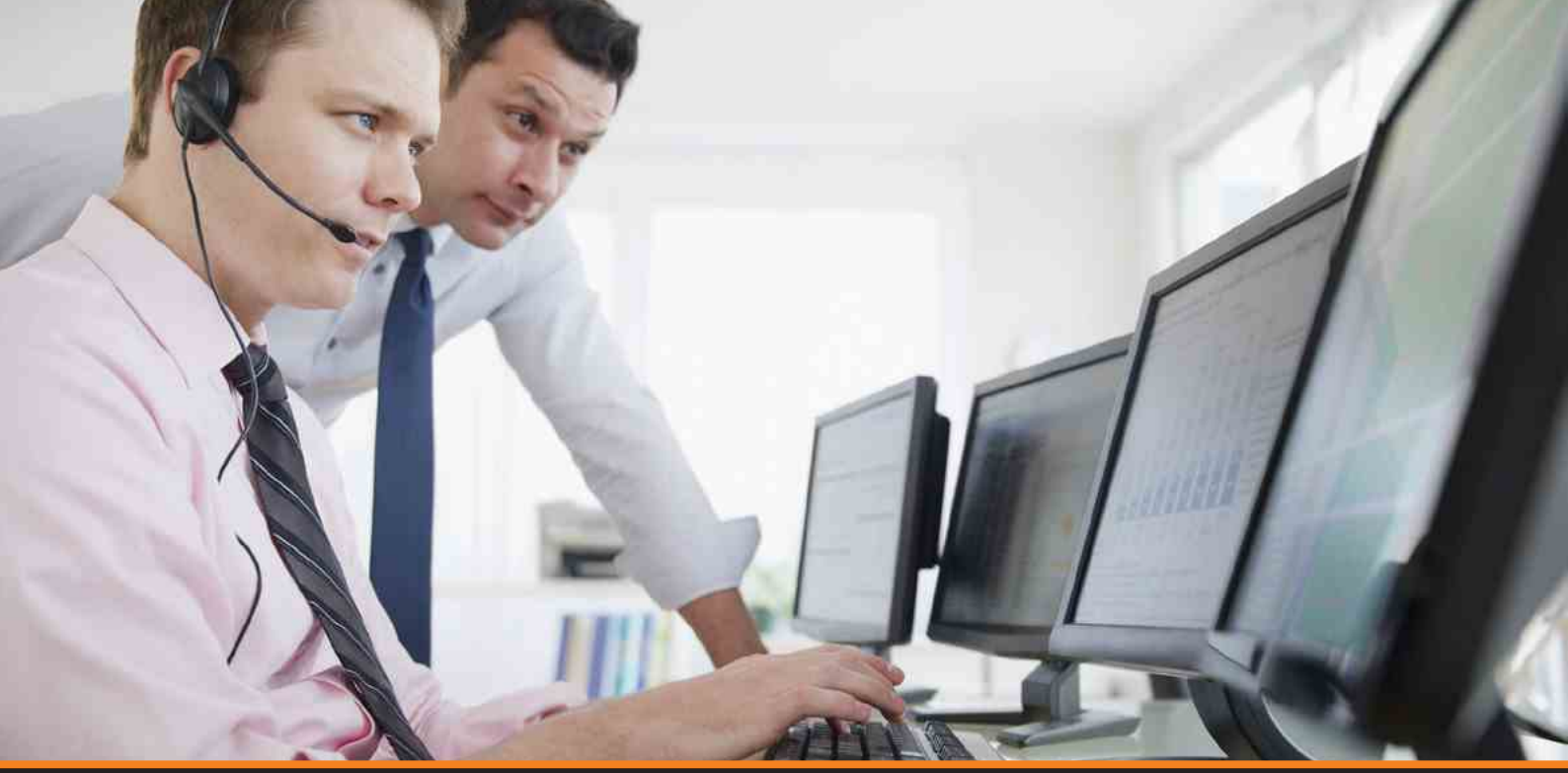
Bang dat hij gehackt wordt en alle gegevens op straat komen

- Ja
- Nee
- Weet het niet



Heeft via werk training gehad om veilig met gegevens om te gaan

- Ja
- Nee
- Weet het niet



Over Orange Cyberdefense

Orange Cyberdefense is de deskundige cybersecurity businessunit van Orange Group en biedt managed security, detectie en respons diensten aan organisaties over de hele wereld. Als dé beveiligingsprovider van Europa streven we ernaar de vrijheid te beschermen en een veiligere digitale samenleving op te bouwen. Wij zijn een bedreigingsonderzoeks- en inlichtingengestuurde beveiligingsprovider die ongeëvenaarde bescherming biedt tegen huidige en opkomende bedreigingen.

Met een trackrecord van meer dan 25 jaar op het gebied van informatiebeveiliging, meer dan 250 onderzoekers en analisten en 16 CyberSOC's verspreid over de hele wereld en verkoop- en servicesondersteuning in 160 landen, kunnen wij wereldwijde bescherming bieden met lokale expertise en onze klanten ondersteunen gedurende de hele levenscyclus van bedreigingen. Voor meer informatie, bezoek https://orangecyberdefense.com/nl/ of volg ons op LinkedIn, Twitter en onze blogs.

Orange is één van 's werelds meest toonaangevende telecommunicatiebedrijven met een omzet van 42,2 miljard euro en 266 miljoen klanten wereldwijd op 31 december 2019. Orange is genoteerd aan de Euronext Parijs (ORA) en aan de New York Stock Exchange (ORAN). In december 2019 presenteerde Orange zijn nieuwe "Engage 2025" strategisch plan, onderbouwd met sociale en ecologische verantwoording. Door de snelle groei in gebieden als B-to-B-diensten en het centraal stellen van data en KI in innovatie, zal de hele Orange Group een aantrekkelijke en verantwoordelijke werkgever zijn.

Orange Cyberdefense
Orteliuslaan 1001
3528 BE Utrecht
088 1234 200
info@orangecyberdefense.nl
www.orangecyberdefense.nl