Digitale vaardigheden van Nederlanders

Onderzoek in opdracht van Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Datum: 25 april 2023

Auteurs: dr. Roxanne van Giesen, Mara Verheijen MSc en dr. Patricia Prüfer

Versie: 3

Classificatie: gevoelig

Uitgave
Centerdata
info@centerdata.nl
www.centerdata.nl

Contact
Roxanne van Giesen
roxanne.van.giesen@centerdata.nl

Inhoudsopgave

Samenvatting

Digitalisering is een groot en complex thema en wordt steeds belangrijker. Er is al veel onderzoek gedaan naar functionele digitale vaardigheden van Nederlanders ("knoppenkennis"). Dit onderzoek focust juist op de meer kritische digitale vaardigheden en maakt gebruik van een innovatieve multi-methodische aanpak waarin naast diepte-interviews en focusgroepen met experts een uitgebreid online vragenlijstonderzoek is uitgezet onder Centerdata's representatieve LISS panel. In dit vragenlijstonderzoek zijn digitale vaardigheden zowel op een subjectieve manier – door te vragen naar eigen percepties van digitale vaardigheden – als op een objectieve manier gemeten. Respondenten moesten verschillende taken uitvoeren waarbij we inzicht kregen in hun daadwerkelijke kritische digitale vaardigheden. Op deze manier kunnen subjectieve percepties van kritische digitale vaardigheden getoetst en geobjectiveerd worden. Hierbij gaat het om informatievaardigheden, zoals het kunnen evalueren van de betrouwbaarheid van informatie; om communicatievaardigheden, ook wel de netiquette; en om content creatie vaardigheden – begrip over hoe online advertenties werken en hoe bepaalde online representaties mensen beïnvloeden.

Het doel van dit onderzoek is om voor de verschillende soorten kritische vaardigheden in kaart te brengen en inzichtelijk te maken tegen welke problematiek verschillende doelgroepen aan lopen. De volgende hoofdvragen staan centraal in dit onderzoek:

- *Welke* (kritische) digitale vaardigheden verschillende subdoelgroepen missen en in welke situaties.
- *Waarom* mensen bepaalde (kritische) digitale vaardigheden missen.
- Welke leerbehoefte er is en *hoe* men graag wil leren.

In de eerste fase vond een kwalitatief vooronderzoek plaats. De input uit deze kwalitatieve fase is gebruikt bij het vormgeven van het online surveyonderzoek in de tweede fase. Vervolgens vond een verdiepende fase plaats, met een focusgroep inclusief design thinking, waarin we met experts de resultaten uit het survey onderzoek duidden en op basis hiervan oplossingsrichtingen en richtingen voor bijscholing bespraken.

Kwalitatief vooronderzoek

In de eerste fase zijn 12 diepte-interviews met verschillende doelgroepen uitgevoerd en vond een focusgroep met experts op het gebied van digitale vaardigheden plaats. Het onderzoek richtte zich in deze fase op het achterhalen van voorbeelden en oorzaken van ontbrekende (kritische) digitale vaardigheden. Uit de kwalitatieve fase bleek dat niet digitaal vaardigen (met name ouderen) niet goed online kunnen bankieren of producten kopen. Ze ervaren angst en blijven hierdoor liever bij het oude vertrouwde, ook al kost dat soms meer moeite.

Digitaal vaardige mensen zijn niet altijd bezig met hun online privacy, wachtwoorden en/of veilige verbindingen. Daarnaast bleek dat ouders met uitgebreide digitale vaardigheden op hun werk, zich vaak minder bewust zijn van wat hun kinderen doen en posten op het internet. Experts signaleren ook dat phishing een toenemend probleem is en het belangrijk is dit thema bespreekbaar te maken om

schaamte en angst te doorbreken. In de kwantitatieve fase is dit verder onderzocht en is ook onderzocht welke doelgroepen minder goed zijn in het herkennen van phishing berichten.

In de kwalitatieve fase zijn daarnaast verschillende oorzaken voor het ontbreken van kritische digitale vaardigheden naar voren gekomen: motorische beperkingen, beperkte kennis, moeilijk leren, laag zelfbeeld, wantrouwen/gebrek aan vertrouwen, schaamte en de culturele context.

Online vragenlijstonderzoek

In de tweede fase van dit onderzoek is een vragenlijst afgenomen in het representatieve LISS panel van Centerdata. De data van 1.392 respondenten werden geanalyseerd. We onderzochten zowel de eigen inschatting van digitale vaardigheden van mensen als de daadwerkelijk (kritische) digitale vaardigheden, door mensen verschillende taken uit te laten voeren. Respondenten kregen verschillende taken voorgelegd die te maken hadden met het gebruik van het internet, om op een meer objectieve manier inzicht te krijgen in de daadwerkelijke kritische digitale vaardigheden.[1] Dit geeft een uitgebreid en uniek beeld van de (kritische) digitale vaardigheden en de problemen waar verschillende doelgroepen tegenaan lopen.

Op basis van het vragenlijstonderzoek bleek dat twee situaties het meest problematisch waren: (1) het herkennen van een nepwebwinkel en (2) het herkennen van phishing mails. Hier gaan we daarom uitgebreider op in.

Het bleek dat mensen *denken* dat ze een nepwebwinkel goed kunnen herkennen, maar dat ze in de praktijk *niet goed nazoeken* of een website echt onbetrouwbaar is, waardoor ze vervolgens in de online taak *de nepwebwinkel niet goed weten te herkennen*. Met name vrouwen en ouderen (65+) hebben meer moeite met het herkennen van de nepwebwinkel. Opvallend is dat opleidingsniveau geen rol speelt. Dat dit een belangrijk probleem is blijkt ook uit het feit dat webshopfraude steeds vaker voorkomt: de politie ontving in 2022 10.500 aangiften over fraude via nepwebshops. Het totale schadebedrag van fraude via nepwebshops was over 2022, al vóór de feestdagen, bijna €4 miljoen (zie website van Politie Nederland).

Ook het herkennen van phishing berichten blijkt lastig te zijn. Men weet niet zo goed onderscheid te maken tussen verschillende soorten berichten (wel of geen phishing). Dat dit ook een serieus probleem is blijkt uit het feit dat in 2021 ruim honderdduizend personen zijn gedupeerd door phishing (zie website van het CBS). Opvallend is dat leeftijd of opleidingsniveau geen rol speelt en dit dus een probleem van alle leeftijden en achtergronden lijkt te zijn.

Als we kijken naar andere kritische informatievaardigheden, zoals het uitvoeren van een zoekopdracht of het herkennen van nepnieuws, blijkt dat een op de 10 respondenten het lastig vindt om een zoekopdracht uit te voeren. Zij vinden het bijvoorbeeld lastig om een zoekmachine te openen of de

[1] Respondenten voerden 3 van de volgende taken uit: een zoekopdracht uitvoeren (kritische informatievaardigheden); een product kopen (kritische informatievaardigheden); het herkennen van nepnieuws (kritische informatievaardigheden); het herkennen van phishing (kritische informatievaardigheden); het adequaat gebruiken van social media (niet voorgelegd aan respondenten die geen social media gebruiken; kritische communicatievaardigheden); vragen omtrent het omgaan met zoekresultaten en een filterbubbel (kritische content creatie vaardigheden).

juiste zoektermen te bepalen. Verder blijkt dat men over het algemeen wel onderscheid kan maken tussen nepnieuws en legitieme nieuwsberichten. Toch vertrouwt ongeveer een vijfde van de respondenten er op dat het online nieuws wel betrouwbaar is en trekt 1 op de 4 een nieuwsbericht *niet* na bij twijfel. Als we kijken naar de kritische communicatievaardigheden dan weet men over het algemeen goed welke berichten men niet zomaar online mag delen zonder dit te vragen.

Sommige mensen zijn digitaal vaardig op één gebied maar missen op andere gebieden digitale vaardigheden. Dit noemen we splintervaardigheden. Uit dit onderzoek komen de volgende splintervaardigheden naar voren bij verschillende subdoelgroepen:

- Vrouwen weten goed een phishing bericht te herkennen maar zijn minder goed in het uitvoeren van een zoekopdracht en het herkennen van een nepwebwinkel, voor mannen is dit precies andersom.
- Jongeren ervaren geen angst en schaamte en weten goed wat ze online wel en niet kunnen delen op social media. Jongeren zijn echter niet zo goed in het herkennen van nepnieuws.
- Lager opgeleiden weten niet zo goed hoe ze een zoekopdracht uit moeten voeren, hoe ze nepnieuws moeten herkennen en hoe ze social media moeten gebruiken.
- Mensen met een migratieachtergrond zijn minder goed in het uitvoeren van een zoekopdracht. Opvallend genoeg hebben zij geen problemen met andere taken zoals het herkennen van nepnieuws.

Wanneer het gaat over bijscholing dan vindt men het belangrijk om meer te leren over het beschermen van de online privacy en over hoe men online fraude kan herkennen. Ook het aanleren van de meer praktische vaardigheden wordt vaker genoemd, zoals het bewerken van foto's en/of video's, het gebruik van een bepaalde programmeertaal en het maken van een website. Over het algemeen gaven jongeren vaker aan een programmeertaal te willen leren en was voor mensen van 35 jaar en ouder het herkennen van online fraude belangrijker. Men leert het liefst via een handleiding op internet, via filmpjes van Youtube of een op een van een vriend of familielid.

Verdiepende fase

Uit dit onderzoek kwamen twee belangrijke problemen naar voren voor de digitale samenleving: mensen zijn niet goed in het herkennen van een nepwebwinkel en het herkennen van phishing berichten. Een aanzienlijk deel van de mensen heeft hier moeite mee. Op deze problemen zijn we daarom in de verdiepende fase uitgebreid ingegaan. Met experts is besproken hoe we kunnen zorgen voor een digitaal inclusieve samenleving waarbij online winkelen en de angst voor nepwebwinkels niet langer een probleem hoeft te zijn. Experts benadrukten dat het lastig is om het bewustzijn van nepwebwinkels bij consumenten te vergroten. Een van de oplossingen die naar voren kwam en breed gedragen werd onder de experts focuste juist op het uitbannen van nepwebshops door alle bedrijven die online producten willen verkopen zicht te laten identificeren (een soort e-herkenning met identificatie op persoonsniveau in plaats van bedrijfsniveau). Andere oplossingen zijn een checklist voor gebruikers zodat men kan controleren of een website betrouwbaar is, meer bewustzijn creëren voor het checken van keurmerken op websites; en campagnes die (ouderen) leren over online winkelen, betalen en online veiligheid.

Ook werd het herkennen van phishing besproken en werd er specifiek gefocust op de urgentie die gevoeld wordt bij het lezen van een phishing mail. Phishing mails komen altijd onverwacht. Hoe kunnen we er nu voor zorgen dat iemand hier niet op klikt? Een van de oplossingen die naar voren kwam en breed gedragen werd onder de experts was een berichtenportal wat rondom het individu is ingericht. Er wordt daarbij dus veel meer gedacht vanuit toestemming van de burger. Daarnaast werden nog tal van andere oplossingen genoemd, zoals een checklist voor gebruikers zodat men kan controleren of een website betrouwbaar is; meer bewustzijn creëren voor het checken van keurmerken op websites; en campagnes die (ouderen) leren over online winkelen, betalen en online veiligheid. Er is vervolgonderzoek nodig om interventies en campagnes, gericht op het herkennen van phishing berichten en nepwebwinkels, goed aan te laten sluiten bij de skills set en het doenvermogen van verschillende groepen burgers.

Dit onderzoek laat zien dat er onder verschillende subdoelgroepen splintervaardigheden voorkomen. Men is dan digitaal vaardiger in één context maar loopt tegen problemen aan in een andere context. Dit onderzoek geeft handvaten om gerichter educatieprogramma's en bewustwordingsstrategieën onder verschillende doelgroepen in te zetten. Zo is het belangrijk om extra aandacht aan lager opgeleiden te geven wanneer het gaat om *alle* (kritische) digitale vaardigheden. Daarnaast is het belangrijk om mensen met een migratieachtergrond (en mogelijk ook een taalachterstand) te ondersteunen met de kritische informatievaardigheden en dan met name het uitvoeren van zoekopdrachten. Dat laatste geldt overigens ook voor mensen met een laag opleidingsniveau.

Bovenal blijkt uit dit onderzoek dat het belangrijk is om te focussen op de twee grootste problemen die ook economisch en financieel aanzienlijk negatieve effecten hebben: het herkennen van phishing berichten en nepwebwinkels. Een aanzienlijk deel van de mensen heeft hier moeite mee maar ziet zelf niet in dat ze hier moeite mee hebben. Veel mensen denken dus dat ze dit goed kunnen, maar kunnen dit in de praktijk niet. In een wereld waarin het aantal nepwebwinkels en phishing berichten toeneemt is het dan ook noodzakelijk om bewustzijn van deze problematiek te vergroten en *alle* mensen digitaal vaardiger te maken op deze vlakken. Wij raden dan ook aan om sterk in te zetten op interventies gericht op het vergroten van bewustwording rondom het herkennen van phishingberichten en nepwebwinkels, of het systeem hier anders op in te richten.

1 Inleiding

1.1 Achtergrond

Digitalisering is een groot en complex thema en wordt steeds belangrijker. Ondanks dat digitalisering kansen biedt voor onze samenleving en economie, zorgt de digitalisering ook voor een digitale kloof en groeiende ongelijkheid in onze samenleving. Goede digitale vaardigheden zijn fundamenteel voor een goed begrip van en deelname aan de huidige en toekomstige samenleving. Maar hoe staat het nu eigenlijk met de digitale vaardigheden van Nederlanders? Er is meer onderzoek nodig naar welke doelgroepen te onderscheiden zijn qua digitale vaardigheden, waar zij tegenaan lopen en hoe je ze het beste bereikt. De centrale onderzoeksvraag is:

Welke vaardigheden ontbreken er in welke context bij mensen die variëren in digitale vaardigheden?

Uit eerder onderzoek blijkt dat digitale vaardigheden in meerdere categorieën zijn onder te verdelen, over veel verschillende domeinen heen gaan en ook op veel verschillende manieren gemeten worden.

In de standaarden en eindtermen van volwasseneducatie wordt een onderscheid in 3 niveaus van digitale vaardigheden gemaakt: instroom, basisniveau 1 en basisniveau 2; voor de volgende domeinen: (1) gebruik van ICT-systemen, (2) beveiliging, privacy en gezondheid, (3) informatie zoeken, (4) informatie verwerken, (5) digitaal communiceren (zie figuur 1.1).

Figuur 1.1 Niveaus van digitale vaardigheden

WAT ZIJN DE NIVEAUS VAN DIGITALE VAARDIGHEDEN?

In de standaarden en eindtermen volwasseneneducatie zijn de niveaus van taal, rekenen en digitale vaardigheden beschreven. Er zijn drie niveaus beschreven voor digitale vaardigheden: Instroom, Basisniveau 1 en Basisniveau 2. Deze niveaus sluiten aan op de niveaus Instroom, 1F en 2F van taal en rekenen.

Niveaus van voorbeelden van digitale vaardigheden

Domeinen	Instroom	Basisniveau 1	Basisniveau 2
Taalniveau	Instroom	1F	2F
Het gebruik van ICT-systemen	telefoon of tablet aanzetten en ontgrendelen, een eenvoudige app gebruiken, pinnen	internet opstarten, bestanden opslaan, foto's maken en sturen	meerdere programma's tegelijk gebruiken, een structuur voor bestanden opzetten
Beveiliging, privacy en gezondheid	wachtwoorden geheim houden, veilige website herkennen, computer afsluiten/uitloggen	veilig wachtwoord maken, begrip van risico's en privacy bij digitaal communiceren	profielinstellingen wijzigen op sociale media zodat alleen bekenden informatie zien
Informatie zoeken	webadressen herkennen, contactgegevens opzoeken op een website	een zoekmachine gebruiken op internet, informatie selecteren op een website	verschillende zoektechnieken gebruiken, informatie beoordelen en selecteren
Informatie verwerken	berichtje typen, eenvoudig digitaal formulier invullen, spellingscorrectie herkennen	eenvoudige tekst typen, informatie in een schema zetten, een bijlage toevoegen aan een bericht	standaard lay-out toepassen, bestanden beheren, online iets bestellen
Digitaal communiceren	een bericht ontvangen en beantwoorden, een online profiel kiezen	berichten met tekst, beeld of geluid maken en doorsturen, een eenvoudige presentatie maken	verschillende communicatiemiddelen kunnen gebruiken voor verschillende doeleinden

Meer informatie over de niveaus is te vinden via www.steunpuntbasisvaardigheden.nl

In het zogenaamde DIGCOM project wordt een indeling in digitale competenties van Nederlanders gemaakt. Hierbij worden verschillende categorieën van digitale vaardigheden onderscheiden, zie tabel 1.1. DIGCOM is gebaseerd op het Europese digitaal competentiekader en *The Youth Digital Skills Indicator*. In het Europese digitaal competentiekader voor consumenten worden verschillende gebieden van digitale vaardigheden beschreven. Binnen deze gebieden vallen weer verschillende kerncompetenties waarbij velerlei voorbeelden van kennis, vaardigheden en attitudes worden gegeven. De belangrijkste worden weergeven in tabel 1.1.

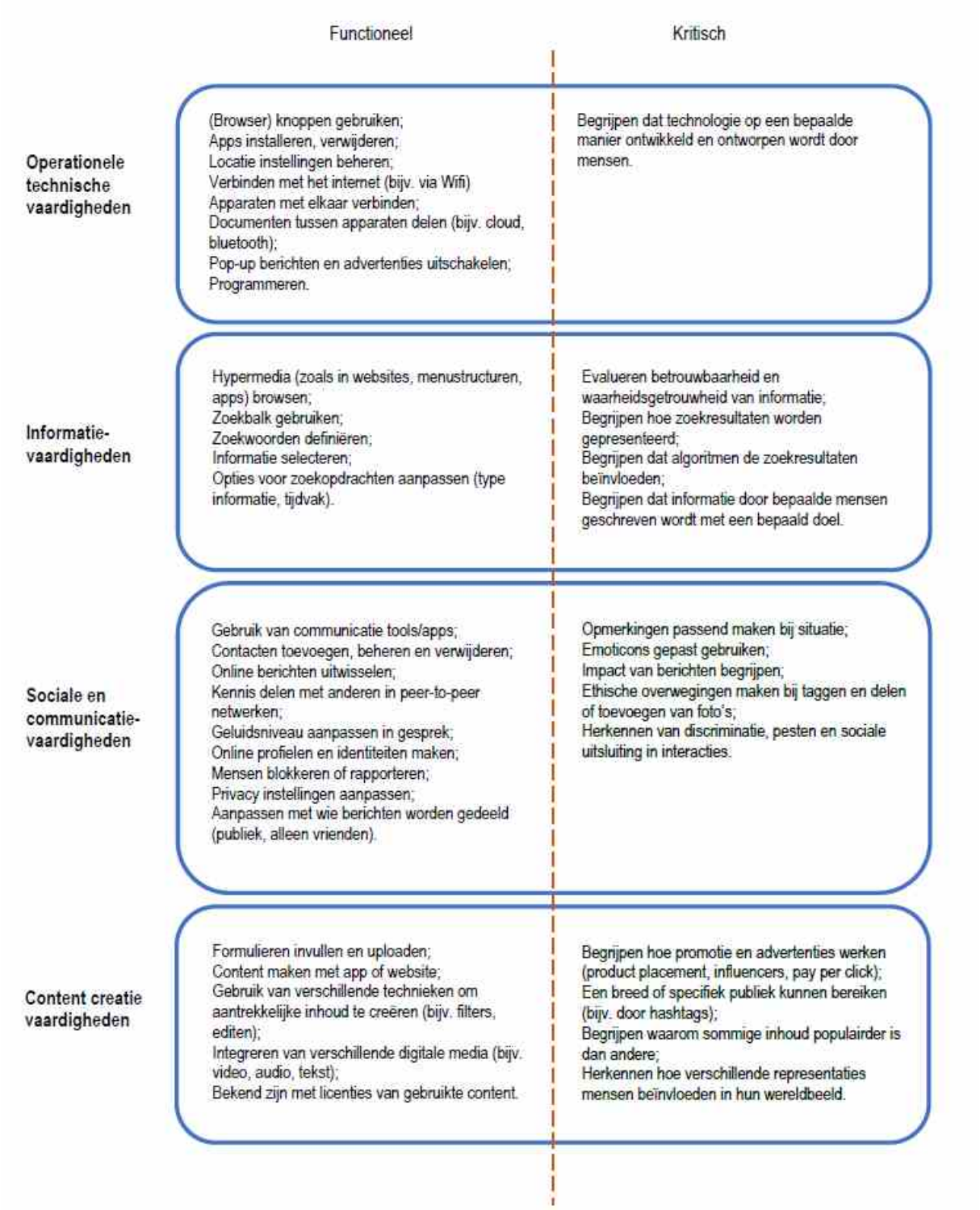
Tabel 1.1 Kerncategorieën/competenties digitale vaardigheden

DIGCOM Dimensies	Beschrijving van relevante competenties
Strategische informatievaardigheden	Informatie zoeken
Kritische informatievaardigheden	Beoordelen van informatie
Netiquette	Op een nette manier omgaan met anderen
Creatieve digitale vaardigheden	Digitale producten maken of kunnen veranderen
Online veiligheid en controle	Digitale gegevens en apparaten kunnen beschermen
Online gezondheid en welzijn	Gezondheid beschermen tegen negatieve gevolgen van internetgebruik
Duurzame/groene digitale vaardigheden	Op een duurzame manier omgaan met digitale apparaten
Digitale problemen oplossen	Weten hoe je hulp kunt krijgen met het internet
AI	Artificiële intelligentie herkennen en ermee om kunnen gaan
DIGCOMP EU Dimensies	**Beschrijving van relevante competenties**
Informatie- en datageletterdheid	Informatie zoeken, evalueren en beheren
Communicatie en samenwerking	Interacteren, delen, samenwerken via digitale technologieën, netiquette en beheer digitale identiteit
Creëren van digitale inhoud	Ontwikkelen, integreren en bewerken digitale inhoud, auteursrecht en programmeren
Veiligheid	Beveiligingsvoorzieningen en bescherming van gegevens (persoonsgegevens, privacy, gezondheid, welzijn, milieu)
Probleemoplossing	Vaststellen van behoeften en antwoorden, creatief gebruik digitale technologieën, kennishiaten

Verder hebben van Deursen en Helsper (2020) uitgebreid onderzoek gedaan naar digitale vaardigheden, zij komen tot vier soorten digitale vaardigheden zoals in het model in figuur 1.2 weergegeven. Deze vaardigheden zijn ook het uitgangspunt voor de eerder genoemde Youth Digital Skills Indicator.

In alle indelingen komt het belang van het kunnen zoeken én beoordelen van informatie terug, het weten hoe men digitaal hoort te communiceren, en of men bewust is van de online veiligheid. De meeste modellen benadrukken daarnaast ook het belang van creëren van digitale inhoud en of maken nog een iets uitgebreider onderscheid in andere aanvullende dimensies, zoals de online gezondheid en het online welzijn. Het model van Deursen en Helsper vat dit mooi samen en is als uitgangspunt gebruikt voor dit onderzoek.

Figuur 1.2. Vier soorten digitale vaardigheden opgesplitst in functionele en kritische vaardigheden (overgenomen van Deursen & Helsper, 2020)



Veel eerder onderzoek focust op de functionele vaardigheden (ook wel de "knoppenkennis"). Het bezit van functionele vaardigheden maakt het uitoefenen van kritische digitale vaardigheden mogelijk. Binnen het huidige onderzoek focussen we juist op de meer kritische vaardigheden:

- **Kritisch operationele vaardigheden:** de manier waarop een platform is ingericht en het begrijpen dat elk platform verschillende technologische karakteristieken heeft die bepaalde soorten acties en reacties uitlokken (bijv. wel of geen optie voor het geven van referenties). Omdat dit (deels) terugkomt bij de andere vaardigheden wordt hier niet als apart onderdeel bij stil gestaan in dit onderzoek.
- **Kritische informatievaardigheden:** dit gaat over het begrijpen hoe zoekresultaten tot stand komen en het evalueren van de betrouwbaarheid van informatie en bronnen.
- **Kritische communicatievaardigheden:** dit wordt ook wel de netiquette genoemd, hoe men online met elkaar om "hoort" te gaan.
- **Kritische content creatie vaardigheden:** hier gaat het om begrip van hoe online advertenties werken, hoe bepaalde representaties mensen beïnvloeden in hun denk- en wereldbeeld. Het gaat ook om het besef dat digitale technologie niet neutraal is.

Sommige mensen hebben bepaalde digitale vaardigheden wel sterk ontwikkeld en andere digitale vaardigheden niet, dit worden *'splintervaardigheden'* genoemd. Ook kan het zo zijn dat men, zodra er iets in de context veranderd, niet meer weet hoe iets werkt. Bijvoorbeeld: wel vaardig zijn met het gebruik van sociale media, maar niet nadenken over de consequenties hiervan. Of, zodra een app een update heeft ondergaan niet meer weten hoe deze app te gebruiken.

In eerder onderzoek zijn (functionele) digitale vaardigheden vaak onderzocht door mensen te vragen of ze bepaalde vaardigheden bezitten in plaats van daadwerkelijk te testen of men digitaal vaardig is. In het huidige onderzoek staan de kritische digitale vaardigheden centraal. In onze innovatieve onderzoeksaanpak vragen we respondenten enerzijds hoe goed zij zelf denken dat hun kritische digitale vaardigheden zijn én anderzijds vragen we ze verschillende taken uit te voeren om hun kritische digitale vaardigheden te testen. Hierdoor kunnen we de subjectieve antwoorden van respondenten objectiveren. We onderzoeken daarnaast welke (kritische) digitale vaardigheden verschillende subdoelgroepen missen en maken inzichtelijk voor welke subgroepen een bepaalde taak (zoals het uitvoeren van een zoekopdracht) extra lastig is. Om dit te achterhalen zijn in dit onderzoek naast een grootschalig vragenlijstonderzoek onder een representatieve steekproef ook diepte interviews en focusgroepen met experts (inclusief design thinking) gebruikt.

1.2 Onderzoeksvragen

Het doel van dit onderzoek is om voor de verschillende soorten kritische vaardigheden in kaart te brengen tegen welke problematiek verschillende subgroepen aan lopen en hoe bewustzijn eventueel vergroot kan worden. Daarbij wordt in dit onderzoek (anders dan in het DigComp onderzoek) vooral gefocust op:

(1) *Welke* (kritische) digitale vaardigheden verschillende subdoelgroepen missen en in welke situaties.
(2) *Waarom* mensen bepaalde (kritische) digitale vaardigheden missen.
(3) Welke leerbehoefte er is en *hoe* men graag wil leren.

1.3 Onderzoeksmethode

Figuur 1.3 geeft een schematisch overzicht van de verschillende onderzoeksfasen. In de eerste fase (november 2022 – januari 2023) vond een kwalitatief vooronderzoek plaats waarin er diepte-interviews onder verschillende type doelgroepen uitgevoerd zijn en een focusgroep met experts op het gebied van digitale vaardigheden plaatsvond. De input uit deze kwalitatieve fase is gebruikt bij het vormgeven van het online surveyonderzoek in de tweede fase (januari 2023 – maart 2023).

Figuur 1.3. Schematisch overzicht onderzoeksfasen

Het interactieve online surveyonderzoek inclusief taken vond plaats onder LISS panelleden van Centerdata. Vervolgens vond een verdiepende fase plaats (maart – april 2023), met een focusgroep inclusief design thinking waarin we met experts de resultaten uit het survey onderzoek duidden en op basis hiervan oplossingsrichtingen en richtingen voor bijscholing bespraken.

In hoofdstuk 2 staat het kwalitatieve vooronderzoek centraal (fase 1), in hoofdstuk 3 het vragenlijstonderzoek (fase 2) en in hoofdstuk 4 de verdiepende fase (fase 3). Hoofdstuk 5 beschrijft de belangrijkste conclusies. In een apart document zijn alle bijlagen behorende bij dit onderzoek te vinden.

2 Fase 1: Kwalitatief onderzoek

In de eerste fase zijn 12 diepte-interviews met verschillende doelgroepen uitgevoerd en vond een focusgroep met experts op het gebied van digitale vaardigheden plaats. Het onderzoek richtte zich in deze fase op het achterhalen van voorbeelden van ontbrekende digitale vaardigheden om zo te achterhalen welke groepen bepaalde splintervaardigheden hebben.

2.1 Diepte-interviews

2.1.1 Methode

In de diepte-interviews werden verschillende oorzaken van onvoldoende digitale vaardigheden en de contexten waarin dit gebeurt in kaart gebracht. Waar lopen mensen tegenaan, in welke situaties gebeurt dit en waarom? Welke digitale uitdagingen ondervinden mensen op het werk en thuis? Ook probeerden we te achterhalen wat hier de oorzaak van kan zijn: ligt dit aan een cognitieve beperking, een motorisch probleem, een gebrek aan vertrouwen in de gevonden informatie en/of toepassingen, een gebrek aan motivatie of zelfvertrouwen, angst, schaamte, en/of de culturele context? En, weten mensen hoe ze hulp kunnen krijgen?

Steekproef

Er werden 12 diepte-interviews uitgevoerd onder Centerdata's LISS panelleden.

In deze stap was het cruciaal een zo gevarieerd mogelijke groep te bevragen, om zoveel mogelijk relevante factoren in kaart te brengen. Tabel 2.1 geeft een overzicht van de type doelgroepen die uitgenodigd waren voor de diepte-interviews.

Tabel 2.1 Aantal deelnemers per doelgroep

Type doelgroep	Aantal
Zeer digitaal vaardig	2
Niet onvaardig, maar ook niet zeer digitaal vaardig:	
- ZZP'ers/ondernemers	2
- Ouders met kinderen tussen de 7 en 14 jaar	2
- Ouderen (tussen de 70 en 75 jaar)	2
Groepen waarbij we op voorhand al bepaalde problematiek kunnen verwachten:	
- Jongeren (tussen de 16 en 19 jaar)	2
- SIMPC gebruikers	2
Totaal	12

Deelnemers werden geselecteerd op basis van een eerder gestelde vraag in het LISS panel over hoe zij omgaan met het beschermen van hun online privacy.[2] Er zijn twee deelnemers uitgenodigd die zeer digitaal vaardig zijn om inzicht te krijgen in welke splintervaardigheden voorkomen bij een meer gevorderde doelgroep en welke nieuwe vaardigheden zij graag zouden leren.

Er zijn zes deelnemers uitgenodigd die een grote groep Nederlanders reflecteren die online best wat kunnen, maar ook dingen lastig vinden. We maken binnen deze groep onderscheid tussen ZZP'ers/ondernemers, ouders met kinderen in de leeftijd van 7 tot 14 jaar en ouderen tussen de 70 en 75 jaar.

Daarnaast zijn er twee jongeren uitgenodigd omdat zij vaak op bepaalde gebieden zeer vaardig zijn, maar de kritische blik op hun online handelen missen. Ook zijn twee SIMPC gebruikers uitgenodigd. Dit zijn LISS panelleden die van Centerdata een eenvoudige PC in bruikleen hebben gekregen en een internetverbinding hebben gekregen om zo de vragenlijsten van Centerdata in te kunnen vullen. Zij missen op veel gebieden digitale vaardigheden.

De interviews vonden plaats op 1, 2 en 5 december 2022. Een interview duurde maximaal een uur en deelnemers kregen een vergoeding van €25 voor deelname. De interviewhandleiding is te vinden in bijlage A.

2.1.2 Belangrijkste resultaten

In deze paragraaf beschrijven we de belangrijkste resultaten uit de diepte-interviews. Een uitgebreidere beschrijving van de resultaten is te vinden in Bijlage B, een aanvullende powerpointrapportage: "Rapportage interviews: Onderzoek digitale vaardigheden".

Welke handelingen / kennis missen specifieke subdoelgroepen en in welke situaties?

Niet digitaal vaardigen (met name ouderen) kunnen niet goed online bankieren of producten kopen. Er leeft vooral **angst**. Ze zijn **bang om gehackt te worden**, bang dat er iemand mee kijkt en/of bang om iets verkeerds te doen en hun geld kwijt te raken. Ze blijven hierdoor liever bij het oude vertrouwde (zonder digitale app), ook al kost dat soms meer moeite (zoals een overschrijvingsformulier bij de bank regelen).

Digitaal vaardigen ervoeren andere uitdagingen. Sommigen hebben een eigen website gebouwd waarbij het niet lukte om alles te programmeren, anderen vinden het lastig om steeds nieuwe software te moeten leren. Ook voor digitaal vaardigen voelt het veiliger om op de computer/laptop administratieve taken of bankzaken te doen. Verder gaven enkele deelnemers aan het lastig te vinden

[2] Privacy protection behaviour, eerder gemeten in het LISS panel en gebaseerd op: Buchanan, Paine, Joinson & Reips (2006); Weinberger, Bouhnik, Zhitomirsky-Geffet (2017) en verder ontwikkeld en gebruikt in een onderzoek voor een Nederlandse internet provider en in een onderzoek voor het Duitse Ministerie van Financiën. Respondenten beantwoordden de vraag: "Op welke manieren beschermt u uw privacy op internet op uw computer/laptop?" Er volgden 17 stellingen variërend van: "ik verwijder of blokkeer cookies" tot "Ik gebruik een privacyvriendelijke zoekmachine zoals bv. DuckDuckGo". Voor deze selectie beschouwen we iemand als zeer digitaal vaardig als men zegt meer dan 15 dingen te ondernemen om de online privacy te beschermen en als "niet onvaardig, maar ook niet zeer digitaal vaardig" als men tussen de 5 en 10 dingen doet om de online privacy te beschermen.

allerlei wachtwoorden te moeten onthouden. Er worden daardoor vaak **standaard wachtwoorden** gebruikt, wat minder veilig is.

Waarom missen mensen vaardigheden en kennis?

Deelnemers die niet digitaal vaardig zijn erkennen dat ze wel mee moeten in de digitale wereld, maar vinden dit lastig. Zij proberen dit wel zoveel mogelijk. Zij maken zich **zorgen over wat ze moeten doen als er geen niet-digitale alternatieven** meer zouden zijn. Ze missen vaak het **begrip** van anderen dat ze niet digitaal vaardig zijn. Dit geeft ze angst en onzekerheid voor de toekomst.

> *De dingen lukken ook op de "ouderwetse manier". Met bellen kom ik al heel ver, betalingen kunnen vaak gewoon nog via pinpas, acceptgiro of overschrijvingsformulier en het inloggen met DigiD heb ik nog nooit hoeven doen. Ik hoef dus ook niet persé nieuwe dingen te leren. Ik vind het allemaal maar een beetje eng en het gaat goed zoals het gaat.* ***(Vrouw, 84)***

Digitaal vaardigen gaven aan niet altijd bezig te zijn met hun **privacy**, wachtwoorden en veilige verbindingen. Ook zijn ze niet altijd bezig met wat hun **kinderen** posten op internet en waar dat allemaal terecht komt. Omdat ze digitaal vaardig zijn lijken ze minder bang voor de *gevaarlijke* kant van het internet.

Welke leerbehoefte hebben mensen en hoe willen ze dit leren?

Er is weinig leerbehoefte bij de deelnemers van de interviews. Ook onder de niet digitaal vaardigen is er weinig interesse om bij te leren, maar zij doen dit wel **uit noodzaak en uit angst** dat het straks niet op een andere manier mogelijk is. Waar mogelijk proberen zij zo lang mogelijk vast te houden aan hoe ze het altijd hebben gedaan. Er is angst voor het onbekende.

Zowel de digitaal vaardigen als de niet digitaal vaardigen geven aan dat zij **geen gebruik maken van cursussen**, de meesten blijven bij door het **gewoon maar te doen**. De niet digitaal vaardigen doen dit met hulp van anderen. De digitaal vaardigen bekijken filmpjes op YouTube, leren van wat anderen op sociale media doen of krijgen hulp van collega's op het werk.

2.2 Focusgroep met experts op het gebied van digitale vaardigheden

Het doel van de focusgroep was om inzicht te krijgen in de problematiek die mogelijk speelt onder verschillende doelgroepen. De focusgroep levert aanvullende inzichten op ten opzichte van de interviews omdat de experts veel meer met digibeten te maken hebben – een groep die niet meegenomen is in de interviews. In deze focusgroep is ingegaan op: oorzaken van onvoldoende digitale vaardigheden en de contexten waarin dit voorkomt.

2.2.1 Methode

In een sessie van 2 uur is met experts van Contour de Twern (Samen Digi-Taal project), de Digi Hulplijn, en Cybersoek gesproken. Deelnemers kregen een vergoeding van €25 voor deelname. Discussies

werden afgewisseld met opdrachten (aan de hand van Padlet). De experts hebben te maken met verschillende doelgroepen, variërend van mensen met een kleine portemonnee, mensen met een migratieachtergrond, en variërend van jong tot oud. De gesprekshandleiding van de focusgroep is te vinden in Bijlage C.

2.2.2 Belangrijkste resultaten

We bespraken met de experts tegen welke digitale uitdagingen mensen aanlopen (bijvoorbeeld thuis, op het werk, of door corona) en mogelijke oorzaken hiervan.

Welke handelingen / kennis missen specifieke subdoelgroepen en in welke situaties?

Een van de uitdagingen die genoemd werd is alles wat met de **corona-situatie** te maken heeft gehad (een combinatie van thuis werken en kinderen die thuis les volgen, en problemen met de coronacheck app). Net als bij de interviews werd hier ook het **gebruik van een DigiD** als uitdaging genoemd. Juist ook veel jongeren blijken vast te lopen bij het gebruik van een DigiD (bijv. uitschrijven van de studie). Bij de DigiHulplijn gaat zo'n 40% van de vragen over de DigiD. Daarnaast is het inmiddels standaard dat er overal wordt verwezen naar een app, bijvoorbeeld als er een trein uitvalt. Dat is onhandig voor mensen die daar niet mee overweg kunnen.

Digitale uitdagingen op het werk zijn bijvoorbeeld: het invullen van de urenregistratie, het downloaden van de loonstrook, het online doorgeven van vakanties. Op het werk hebben mensen daarnaast soms moeite met bepaalde software of het aanleren van de systemen. Ook bij jongeren zijn veel computervaardigheden niet goed, omdat ze voornamelijk met tablets/smartphones werken waar alles erg intuïtief is. Kinderen die opgroeien zonder een computer thuis of een laptop op school kunnen vaak niet met desktops en programma's zoals Microsoft Office werken.

Phishing is een toenemend probleem. Er is een piek in phishingberichten waar te nemen rondom belangrijke momenten waarop de Belastingdienst brieven uitstuurt. Ook gebeurt er veel phishing via de telefoon, waarbij mensen worden gebeld door hun bank en zeer realistisch en professioneel worden misleid. Fraudeurs weten de kwetsbare mensen goed te vinden. Een voorwaarde om te kunnen controleren of informatie betrouwbaar is, is het taalniveau en het begrijpend kunnen lezen. Daarnaast weten mensen vaak helemaal niet waar ze op moeten letten. De experts geven aan dat het belangrijk is om uit te leggen waar mensen op moeten letten, kritisch te blijven op wat men ontvangt en bij twijfel de instantie contacteert. Ze benadrukken tot slot dat het belangrijk is het thema bespreekbaar te maken en de schaamte en angst te doorbreken (phishing kan iedereen overkomen).

De experts denken ook dat het essentieel is dat **kinderen diverse digitale vaardigheden aanleren**, zoals omgaan met Microsoft Office producten, dingen opzoeken op internet, typen, toetsenbordfuncties, herkennen van nepnieuws, tools aangereikt krijgen hoe om te gaan met online pesten en social media gebruik.

Waarom missen mensen vaardigheden en kennis?

- Belangrijke oorzaken voor het ontbreken van digitale vaardigheden zijn:
- Motorische beperkingen (o.a. muisgebruik, kleine lettertjes op de smartphone, toegankelijkheid voor visueel beperkten).
- Beperkte kennis of gebrek aan specifieke kennis van een onderwerp. Dit zorgt er ook voor dat men onzeker is en angst ervaart.
- Moeilijk kunnen leren.
- Laag zelfbeeld.
- Mensen met een psychische kwetsbaarheid zijn vaak wantrouwend ten opzichte van digitale zaken.
- Er is een gebrek aan vertrouwen in informatie, vaak als het gaat over dingen als phishing.
- Er heerst schaamte onder mensen die altijd een trucje hebben geleerd en daarin de ontwikkelingen op het gebied van ICT niet hebben kunnen bijbenen. Mensen durven vaak geen hulp te vragen. Ze zijn bang dat men niet de tijd neemt om iets uit te leggen of bang voor reacties als: “snap jij dat niet?”.
- Ook de culturele context speelt een rol. Een taalachterstand/onvoldoende Nederlandse taalbeheersing maakt het lastig om digitale begrippen te begrijpen. Het is dan belangrijk om eerst de taal beter te leren voordat digitale vaardigheden aangeleerd kunnen worden. Echter worden de digitale vaardigheden steeds urgenter.

De experts concluderen dat het allemaal steeds complexer wordt en het basisniveau (bijv. begrijpelijke taal) dat gevraagd wordt steeds hoger wordt. Een taalachterstand is niet nieuws, maar de groep die (grote) problemen heeft, wordt steeds groter. Ze merken daarnaast dat digitale vaardigheden minder prioriteit hebben bij een groep die het toch al lastig heeft. Mensen zijn dan vooral bezig met financiële kwesties (schulden) en hun werk, pas veel later in het lijstje komt het ontwikkelen van digitale vaardigheden.

2.3 Conclusies en aanbevelingen voor fase 2

Uit de kwalitatieve fase bleek dat niet digitaal vaardigen (met name ouderen) niet goed online kunnen bankieren of producten kopen. Ze ervaren angst en blijven hierdoor liever bij het oude vertrouwde, ook al kost dat soms meer moeite.

Digitaal vaardige mensen kunnen online een hoop, zoals het regelen van administratieve zaken, het doen van online aankopen, het gebruik van software voor het werk; echter zijn ze niet altijd bezig met hun online privacy, wachtwoorden en/of veilige verbindingen. Daarnaast bleek dat ouders met uitgebreide digitale vaardigheden op hun werk, zich vaak minder bewust zijn van wat hun kinderen doen en posten op het internet. Experts signaleren ook dat phishing een toenemend probleem is en het belangrijk is dit thema bespreekbaar te maken om schaamte en angst te doorbreken. In de kwantitatieve fase is het daarom belangrijk dit verder te onderzoeken en ook in te zoomen op welke doelgroepen er minder goed zijn in het herkennen van phishing berichten. Ook gaan we in de vragenlijst verder in op het online gedrag van kinderen (voor ouders met kinderen).

In de kwalitatieve fase zijn verschillende factoren genoemd die kunnen verklaren waarom kritische digitale vaardigheden ontbreken of op sommige gebieden wel aanwezig zijn maar niet op andere gebieden (splintervaardigheden): motorische beperkingen, beperkte kennis, moeilijk leren, laag zelfbeeld, wantrouwen/gebrek aan vertrouwen, schaamte, culturele context. Deze aspecten worden (deels) meegenomen in de kwantitatieve fase en gebruikt om te onderzoeken of dit voorspelt waarom iemand een bepaalde taak wel of niet goed uit kan voeren (bijv. het herkennen van phishing berichten).

3 Fase 2: online surveyonderzoek

3.1 Onderzoeksmethode

3.1.1 Steekproefkenmerken

In februari 2023 is een vragenlijst afgenomen in het representatieve LISS panel van Centerdata. Het LISS panel is bij uitstek geschikt voor onderzoek waarbij een goede vertegenwoordiging van de Nederlandse bevolking van groot belang is. Het LISS panel is een probability-based panel (geen zelfselectie mogelijk) van ongeveer 4,600 huishoudens die iedere maand vragenlijsten invullen via internet. De adressensteekproeven voor de werving en de bijwervingen zijn getrokken uit het populatieregister in samenwerking met het CBS. Indien een huishouden niet beschikt over een breedbandverbinding en/of computer, dan stelt Centerdata de benodigde apparatuur in bruikleen beschikbaar om alsnog mee te kunnen doen aan het panel. Hiermee onderscheidt het LISS panel zich van andere online panels, waar niet-internetters ontbreken en waar panelleden de gelegenheid hebben om zichzelf aan te melden. Verder wordt er in het LISS panel ook veel aandacht besteedt aan de begrijpelijkheid van de vragenlijst voor alle lagen van de Nederlandse bevolking. De vragenlijst wordt daarom opgesteld in B1-taalniveau.

Tabel 3.1. Steekproefkenmerken (*N* = 1.392)[3,4]

	Steekproef	Nederlandse bevolking (CBS, jan 2021)
Geslacht		
Man	51,1%	49,3%
Vrouw	48,9%	50,7%
Leeftijd		
16-24	12,6%	10,9%
25-34	17,9%	15,9%
35-44	16,2%	14,7%
45-54	16,7%	17,1%
54-64	15,2%	17,0%
65+	21,4%	24,4%
Opleiding (*N* = 1.384)		
Basisonderwijs	5,8%	8,6%
(V)MBO	35,9%	46,8%
HAVO/VWO	11,8%	8,7%
HBO	22,8%	22,4%
WO	29,1%	13,4%

[3] De initiële selectie van respondenten is zo gemaakt dat deze zoveel mogelijk een weerspiegeling van de Nederlandse bevolking is.
[4] *n* = 1.384 voor opleiding; de 8 overige respondenten hadden (nog) geen onderwijs afgerond of gaven aan dat iets anders van toepassing was.

Niet digitaal vaardigen (alsook mensen met een taalniveau lager dan B1) zijn *niet* meegenomen in dit onderzoek. Er is immers al veel bekend over deze doelgroep(en) en verschillende organisaties bieden al oplossingen of hulp aan, specifiek gericht op verschillende niet digitale doelgroepen.

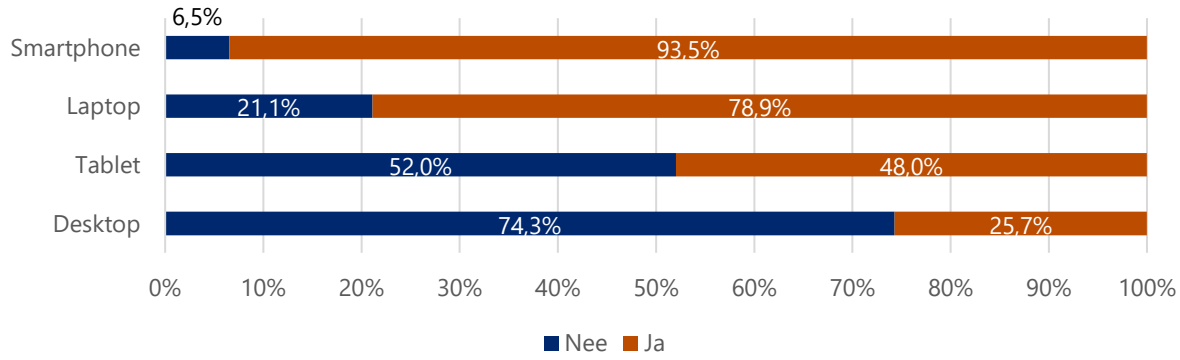
De invulduur van de vragenlijst was 15 minuten (mediaan). De volledige vragenlijst (inclusief literatuurverwijzingen) is te vinden in bijlage D. Respondenten die minder dan 5 minuten deden over het invullen van de vragenlijst zijn niet meegenomen in de analyses. Het totale aantal respondenten komt daarmee op **1.392**. Tabel 3.1 geeft een overzicht van de steekproefkenmerken.

3.1.2 Vragenlijst digitale vaardigheden

We vroegen eerst welke apparaten respondenten thuis allemaal gebruiken:

- 93,5% gebruikt een smartphone;
- 78,9% gebruikt een laptop;
- 48,0% gebruikt een tablet;
- 25,7% gebruikt een desktop (zie figuur 3.1).

Figuur 3.1 Gebruik apparaten



Eigen inschatting digitale vaardigheden en oorzaken

In het vragenlijstonderzoek werden vervolgens knoppenkennis, een inschatting van eigen digitale vaardigheden, privacy attitude, kritische digitale vaardigheden (informatie, communicatie en content creatie) en oorzaken voor ontbrekende digitale vaardigheden (vertrouwen, angst, schaamte) gemeten op 5-puntsschalen en allemaal met minstens 3 items. Hierna werd het gemiddelde genomen van de items behorend bij een bepaald concept. Uit de betrouwbaarheidsanalyses bleek dit goed te gaan voor bijna alle concepten, behalve kritische content creatie vaardigheden (zie bijlage E voor Cronbach's alfa per construct). In het geschatte model zijn daarom alleen de kritische content vaardigheden meegenomen.

Digitale vaardigheden bij het uitvoeren van taken

Na de eigen inschatting van digitale vaardigheden en oorzaken van ontbrekende digitale vaardigheden kregen respondenten verschillende taken voorgelegd die te maken hebben met het

gebruik van het internet, om op deze manier inzicht te krijgen in de daadwerkelijke kritische digitale vaardigheden.

Waar respondenten eerder in de vragenlijst *zelf* aangaven (dus *subjectief*) in hoeverre ze iets wel of niet kunnen, meten we hier op een *objectieve* manier of het wel of niet lukt om een bepaalde taak uit te voeren.

Respondenten werden random toegewezen aan 3 van de volgende taken:

- een zoekopdracht uitvoeren (kritische informatievaardigheden);[5]
- een product kopen (kritische informatievaardigheden);
- het herkennen van nepnieuws (kritische informatievaardigheden);
- het herkennen van phishing (kritische informatievaardigheden);[6]
- het adequaat gebruiken van social media (niet voorgelegd aan respondenten die geen social media gebruiken; kritische communicatievaardigheden);[7]
- vragen omtrent het omgaan met zoekresultaten en een filterbubbel (kritische content creatie vaardigheden).[8,9]

Bijscholing, digitale vaardigheden van kinderen en achtergrondkenmerken

We onderzochten de leerbehoefte van respondenten. We vroegen wat respondenten nog beter willen leren op het gebied van digitale vaardigheden, variërend van routes plannen via Google maps tot het herkennen van online fraude. Vervolgens vroegen we hoe ze dit graag willen leren, bijvoorbeeld 1 op 1 van een vriend of familielid, via filmpjes van Youtube of een handleiding op internet.

Aan de respondenten met thuiswonende kinderen, in de leeftijd van 7 tot 15 jaar, vroegen we welke social media hun kinderen gebruiken, welke afspraken gemaakt zijn over het online gedrag van de kind(eren) en of en waarmee men zelf wel eens geholpen wordt door de kinderen met online zaken.

Via een aantal (kern)vragenlijsten[10] die met regelmaat in Centerdata's online panel worden afgenomen is er een grote database beschikbaar met achtergrondkenmerken van panelleden. Voor dit onderzoek hebben we de antwoorden van panelleden gekoppeld aan enkele van deze eerder gemeten demografische gegevens (geslacht, leeftijd, opleiding, regio, stedelijkheid, migratieachtergrond, religie, thuis geen Nederlands spreken, ZZP'er, of iemand wel of niet studeert, of iemand wel of geen partner heeft).

[5] Gebaseerd op Youth Skills vragenlijst
[6] Gebaseerd op: Emma J Williams, Adam N Joinson, Developing a measure of information seeking about phishing, Journal of Cybersecurity, Volume 6, Issue 1, 2020, en Kleitman S, Law MKH, Kay J (2018) It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. PLoS ONE 13(10): e0205089.
[7] Gebaseerd op Youth Digital Skills vragenlijst
[8] Geabseerd op eerder onderzoek van Centerdata voor het Duitse Ministerie van Financiën.
[9] Het is in het vragenlijstonderzoek niet mogelijk om taken op te nemen die over andere content creatie vaardigheden gaan (bijv. het vergroten van social media bereik), daarom is dit deels uitgevraagd aan de hand van stellingen.
[10] Link naar website Centerdata

3.2 Resultaten

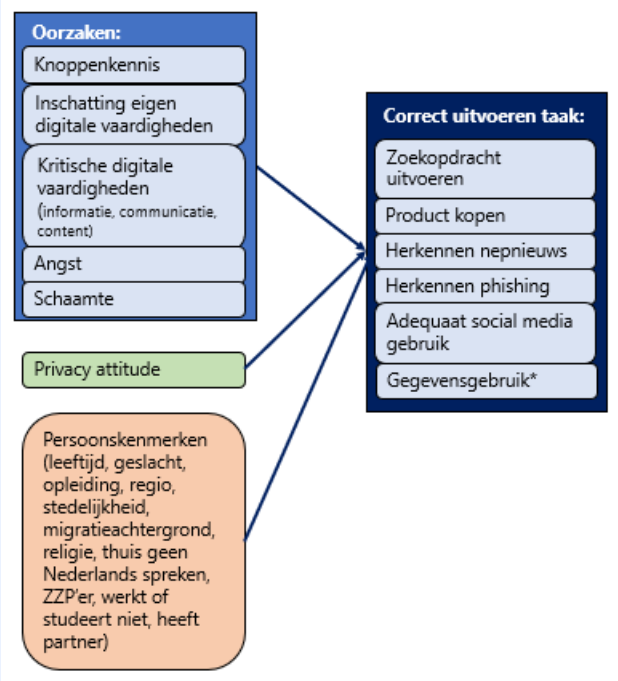
Tabel 3.2 beschrijft waar de analyses zich op richten. De beschrijvende analyses geven inzicht in het percentage van de mensen dat bepaalde kennis of vaardigheden mist voor verschillende situaties (onderzoeksvraag 1). Ook geven de beschrijvende analyses inzicht in de leerbehoefte die mensen hebben en hoe ze dat graag willen leren (onderzoeksvraag 3). Met de statistische analyses geven we inzicht in of - onderliggende oorzaken, persoonskenmerken of attitudes een rol spelen bij het uitvoeren van taken (onderzoeksvraag 2). Het model in figuur 3.2 toont het model dat steeds per taak geschat is. Tot slot voeren we analyses per subgroep uit (onderzoeksvraag 2). We onderzoeken dan of specifieke subgroepen meer moeite hebben met het uitvoeren van een bepaalde taak. Dit geeft inzicht in de splintervaardigheden.

Tabel 3.2 Analyses om inzicht te geven op de onderzoeksvragen

	Analyse	Antwoord op de vraag
Stap 1	Beschrijvende analyses - scenario's - vragenlijst	Hoeveel % van de mensen kiest een bepaald antwoord? Bijvoorbeeld: Hoeveel % van de mensen kan een bepaalde taak uitvoeren (zoals het uitvoeren van een zoekopdracht? Hoeveel % van de mensen zou graag bij willen leren over online privacy? Hoeveel % van de mensen zou graag een online cursus willen volgen om bij te leren over een bepaald thema?
Stap 2	**Statistische analyses**	
Stap 2a	Samenhang tussen (1) uitvoeren van een taak, (2) oorzaken; (3) privacy attitude; (4) persoonskenmerken	In welke mate is het kunnen uitvoeren van de taken te voorspellen op basis van (1) onderliggende oorzaken (knoppenkennis, angst, schaamte, privacy attitude, kritische digitale vaardigheden, inschatting eigen digitale vaardigheden, persoonskenmerken (geslacht, leeftijd, opleiding, regio, stedelijkheid, migratieachtergrond, religie, thuis geen Nederlands spreken, ZZP'er, of iemand wel of niet studeert, of iemand wel of geen partner heeft)?
Stap 2b	Analyse per subgroep (geslacht, leeftijd, opleiding, regio, stedelijkheid, migratieachtergrond, religie, thuis geen Nederlands spreken, ZZP'er, of iemand wel of niet studeert, of iemand wel of geen partner heeft)	Hoe verschilt het kunnen uitvoeren van een taak tussen bepaalde subgroepen? Welke groepen verdienen speciale aandacht?

Figuur 3.2 Onderzoeksmodel

In welke mate is de reactie van consumenten in concrete situaties waarbij kritische digitale vaardigheden getest worden te voorspellen op basis van (1) knoppenkennis, inschatting eigen digitale vaardigheden, kritische digitale vaardigheden, angst, schaamte, (2) het belang dat ze (zeggen te) hechten aan privacy (privacy attitude) en (3) andere persoonskenmerken (leeftijd, geslacht, opleiding, regio, stedelijkheid, migratieachtergrond, religie, thuis geen Nederlands spreken, ZZP'er, of iemand wel of niet werkt of studeert, of iemand wel of geen partner heeft)? Om deze vraag te beantwoorden hebben we per taak een logistisch regressiemodel geschat met het correct uitvoeren van de taak als afhankelijke variabele en indicatoren voor oorzaken van (ontbrekende) digitale vaardigheden, privacy attitude en de persoonskenmerken als verklarende factoren. Als een effect significant is ($p < 0{,}05$) wil dat zeggen dat het percentage dat de taak correct uitgevoerd heeft anders is wanneer men bijvoorbeeld veel versus weinig knoppenkennis heeft. Het is dan zeer onwaarschijnlijk dat het waargenomen verschil aan toeval te wijten is. De *p-waarden* worden in voetnoten gerapporteerd. Een *M* staat voor gemiddelde en een *n* voor de groepsgrootte.



Noot: bij gegevensgebruik gaat het niet om het correct uitvoeren van de taak, maar om de antwoorden op de stellingen.

3.2.1 Eigen inschatting digitale vaardigheden en oorzaken

Bijna de helft van de respondenten is (heel erg) **bezorgd** dat persoonlijke informatie gebruikt wordt door de overheid en is zelfs nog iets bezorgder dat dit door bedrijven gebruikt wordt (overheid: 47,5%, bedrijven: 61,1%). Slechts 6,2% en 3,2% van de respondenten is hier helemaal niet bezorgd over. Mensen ouder dan 35 jaar zijn over het algemeen bezorgder over het gebruik van hun persoonlijke informatie.[11]

In het algemeen zien we dat de **knoppenkennis hoog is**. Knoppenkennis is een vereiste voor de meer kritische digitale vaardigheden. Het merendeel van de respondenten (meer dan 94,8%) kan een e-mail versturen, een bestand/bijlage openen, een tekstbericht versturen, een internetbrowser vinden en

[11] $p < 0{,}001$; 55-64 jarigen en 65+ waren significant bezorgder over hun privacy ($M = 3{,}86$ en $M = 3{,}98$) dan de andere leeftijdscategorieën (alle p's $< 0{,}002$). Jongeren van 16-24 jaar en 25-34 jaar waren minder bezorgd ($M = 3{,}31$ en $M = 3{,}52$) dan de andere leeftijdscategorieën (alle p's $< 0{,}05$; er was geen significant verschil tussen 25-34 jaar en 35-44 jaar ($M = 3{,}59$). Ook stedelijkheid heeft een significant effect, $p = 0{,}034$.

openen en een bestand als bijlage aan een e-mail toevoegen. Voor minder dan 2,5% is het (erg) lastig om deze dingen uit te voeren.

Wanneer respondenten hun **eigen digitale vaardigheden** in moeten schatten blijkt dat het grootste deel van de respondenten géén moeite heeft met het overmaken van geld via internetbankieren (96,6%) en het inloggen met een DigiD (96,6%).[12] 29,0% van de respondenten vindt het lastig om privé browsen te gebruiken. Slechts iets meer dan 10% van de respondenten kan een programmeertaal gebruiken.

Kritische digitale vaardigheden

De **kritische digitale vaardigheden** zijn onderverdeeld in informatievaardigheden, communicatievaardigheden en content creatie vaardigheden. Wanneer het gaat om **kritische informatievaardigheden** weet bijna 80% of meer de beste zoekwoorden voor online zoekopdrachten te kiezen, in de browsergeschiedenis een website te vinden die eerder bezocht is en de uitgebreide zoekfuncties in zoekmachines te gebruiken. (Bijna) 70% weet te bepalen of een website te vertrouwen is en te controleren of de informatie die online gevonden wordt waar is.

Wanneer het gaat om **kritische communicatievaardigheden** weet meer dan 80% wanneer het gepast is om emoticons te gebruiken en hoe de microfoon uit te zetten of het beeld uit te schakelen in online gesprekken. Meer dan 60% weet gesponsorde van niet-gesponsorde berichten te onderscheiden, hoe ze negatieve reacties op social media moeten melden en hoe te verwijzen naar inhoud van iemand anders. Iets meer dan de helft weet te herkennen wanneer iemand online gepest wordt.

Wanneer het gaat om **kritische content creatie vaardigheden** weet meer dan 70% dat bedrijven gewone mensen betalen om hun producten te gebruiken in de video's of foto's die ze online plaatsen. Verder weet 60% of meer dat het eerste zoekresultaat van een online zoekmachine niet altijd de beste informatiebron is en dat niet iedereen dezelfde zoekresultaten te zien krijgt wanneer via een online zoekmachine naar dingen wordt gezocht. Iets meer dan de helft weet dat het gebruik van hashtags de zichtbaarheid van een online bericht vergroot. En iets minder dan de helft weet dat het eerste bericht op een sociale media tijdlijn niet altijd als laatste door een van zijn/haar contacten geplaatst is.

Over het algemeen blijkt dat mannen, jongeren, hoger opgeleiden en mensen die werken of studeren hun eigen digitale vaardigheden hoger inschatten. ZZP'ers schatten bovendien hun kritische content vaardigheden hoger in. Daarnaast blijkt dat mensen met een migratieachtergrond en mensen die religieus zijn hun eigen digitale vaardigheden lager inschatten.[13]

[12] Het gaat hier om helemaal eens en een beetje eens bij elkaar opgeteld. Dat geldt ook voor de resultaten die in de rest van deze paragraaf besproken worden.

[13] Alle *p's* < 0,05 voor geslacht, opleidingsniveau, leeftijdscategorie, werkt of studeert niet, migratieachtergrond; voor de inschatting van de eigen digitale vaardigheden. Alle *p's* < 0,05 voor geslacht, opleidingsniveau, leeftijdscategorie, werkt of studeert niet, religie; voor de inschatting van de kritische informatievaardigheden. Alle *p's* < 0,05 voor geslacht, opleidingsniveau, leeftijdscategorie, werkt of studeert niet, religie; voor de inschatting van de kritische communicatievaardigheden. Alle *p's* < 0,05 voor geslacht, opleidingsniveau, leeftijdscategorie, thuis geen Nederlands spreken, migratieachtergrond, ZZP'er; voor de inschatting van de content vaardigheden.

Mogelijke oorzaken van ontbrekende digitale vaardigheden

We onderzochten ook of men (gebrek aan) vertrouwen heeft in het internet, of men angst heeft om online iets verkeerds te doen en of men schaamte ervaart voor de dingen die mogelijk online niet lukken. Iets meer dan 1 op de 10 respondenten heeft **weinig vertrouwen** in de informatie die op internet te vinden is en/of vermijd het gebruik van internet. Bijna een derde van de respondenten ervaart **angst,** bijvoorbeeld omdat iemand geld kan stelen als ze online persoonlijke gegevens afstaan of over dat zijn/haar apparaat wordt gehackt. Zo'n 1 op de 5 respondenten is vaak bezorgd dat ze online iets verkeerds doen en dat nadelige gevolgen heeft, dat zijn/haar online identiteit misbruikt wordt, dat ze slachtoffer worden van fraude met online bankieren of dat de dingen die ze online bestellen niet bezorgd worden. Tot slot blijkt dat minder dan 1 op de 10 respondenten **schaamte** ervaart omdat zij niet weten hoe ze iets op een bepaald apparaat moeten doen. Minder dan 5% van de respondenten durft geen hulp te vragen en/of wil niet dat anderen te weten komen dat ze iets online niet kunnen. Over het algemeen blijkt dat vrouwen, 55+'ers, lager opgeleiden, mensen met een migratieachtergrond, mensen die thuis geen Nederlands spreken en mensen die niet werken of studeren meer angst ervaren; en dat lager opgeleiden, mensen met een migratieachtergrond, mensen die niet werken of studeren en mensen zonder partner meer schaamte ervaren wanneer het gaat om hun digitale vaardigheden. Mensen in de leeftijd van 25-34 jaar ervaren het minste schaamte om hun eigen digitale vaardigheden.[14]

Bijlage F geeft nog meer achtergrondinformatie over de eigen inschatting van digitale vaardigheden en oorzaken.

3.2.2 Digitale vaardigheden bij het uitvoeren van taken

Een zoekopdracht uitvoeren

Respondenten moesten een nieuw venster openen en **een zoekmachine gebruiken** om antwoord te geven op de vraag wat de warmste junimaand ooit was in Nederland. Ook moesten zij opzoeken wat de gemiddelde temperatuur in de warmste junimaand ooit gemeten was in De Bilt.

78,5% van de respondenten **denkt** het goede antwoord op beide vragen te hebben gegeven en 49,3% **gaf daadwerkelijk** de goede antwoorden.[15] Verder had:

- 21,3% beide vragen fout beantwoord
- 17,5% een van de vragen goed beantwoord
- 4,0% het antwoord op een van de vragen niet kunnen vinden
- 7,9% het antwoord op beide vragen niet kunnen vinden.

84,7% van de respondenten vond het een (hele) makkelijke zoekopdracht.

[14] Angst: *p's* < 0,05 voor geslacht, leeftijdscategorie, opleidingsniveau laag, migratieachtergrond, thuis geen Nederlands spreken, niet werken of studeren; Schaamte: *p's* < 0,05 voor opleidingsniveau laag en leeftijdscategorie, migratieachtergrond. Daarnaast blijkt dat mensen die in Noord-Nederland (Groningen, Friesland, Drenthe) wonen iets meer schaamte ervaren omtrent de eigen digitale vaardigheden dan mensen die in andere regio's van Nederland wonen.
[15] n = 680.

11,5% van de respondenten had de zoekopdracht **niet uitgevoerd**. Als we deze groep respondenten uit de analyse laten zien we een vergelijkbaar patroon. 87,5% van de respondenten **dacht** het goede antwoord op beide vragen te hebben gegeven en 55,6% gaf daadwerkelijk de goede antwoorden.[16]

De respondenten die bij de eerste vraag aangaven dat ze het antwoord niet konden vinden werden gevraagd in hoeverre zij het lastig vonden om een zoekmachine te openen en de zoektermen te bepalen.[17] Voor 39,5% van deze respondenten was het **lastig om een zoekmachine te openen** en voor 34,6% was het lastig om **de juiste zoektermen te bepalen**.

Tot slot blijkt dat **lager opgeleiden meer moeite** hebben met het uitvoeren van de zoekopdracht.[18] Namelijk 33,7% van de lager opgeleiden gaf het goede antwoord vergeleken met 60,6% met een midden/hoog opleidingsniveau.[19] **Vrouwen** zijn minder goed in het uitvoeren van de zoekopdracht dan mannen (51,6% vs. 59,7%). Ook zien we dat de **kritische content vaardigheden** een rol spelen.[20] Dit gaat onder andere over of men denkt dat het eerste zoekresultaat de beste informatiebron is en of iedereen dezelfde zoekresultaten te zien krijgt. Mensen die de zoekopdracht correct uitvoerden scoorden gemiddeld hoger op kritische content creatie vaardigheden (M = 3,0) dan mensen die de vraag fout hadden (M = 2,5). Verder speelt **stedelijkheid** een rol: mensen die in stedelijke gebieden wonen zijn iets minder goed in het uitvoeren van een zoekopdracht (51,6% vs. 59,9%).[21] Ook blijkt dat mensen met een **migratieachtergrond** minder goed zijn in het uitvoeren van de zoekopdracht (38,9%) dan autochtone Nederlanders (59,5%).[22]

Een product kopen

Respondenten stelden zich voor dat zij in een webwinkel een televisie gingen koppen. Zij kregen vier aanbieders te zien en moesten aangeven welke website volgens hen het *minst* betrouwbaar was. Om herkenning van grote bestaande aanbieders (zoals Coolblue of Mediamarkt) te voorkomen werden minder bekende webwinkels getoond. De nepwebwinkel kwam uit een lijst van nepwebshops van de Consumentenbond.[23]

24,1% van de respondenten wist niet welke van de aanbieders het minst betrouwbaar was.[24] Als we deze groep niet meenemen dan wist 25,8% de nepwebwinkel als minst betrouwbaar aan te wijzen en 74,2% gaf een van de andere webwinkels aan als minst betrouwbaar, zie figuur 3.3.[25] De

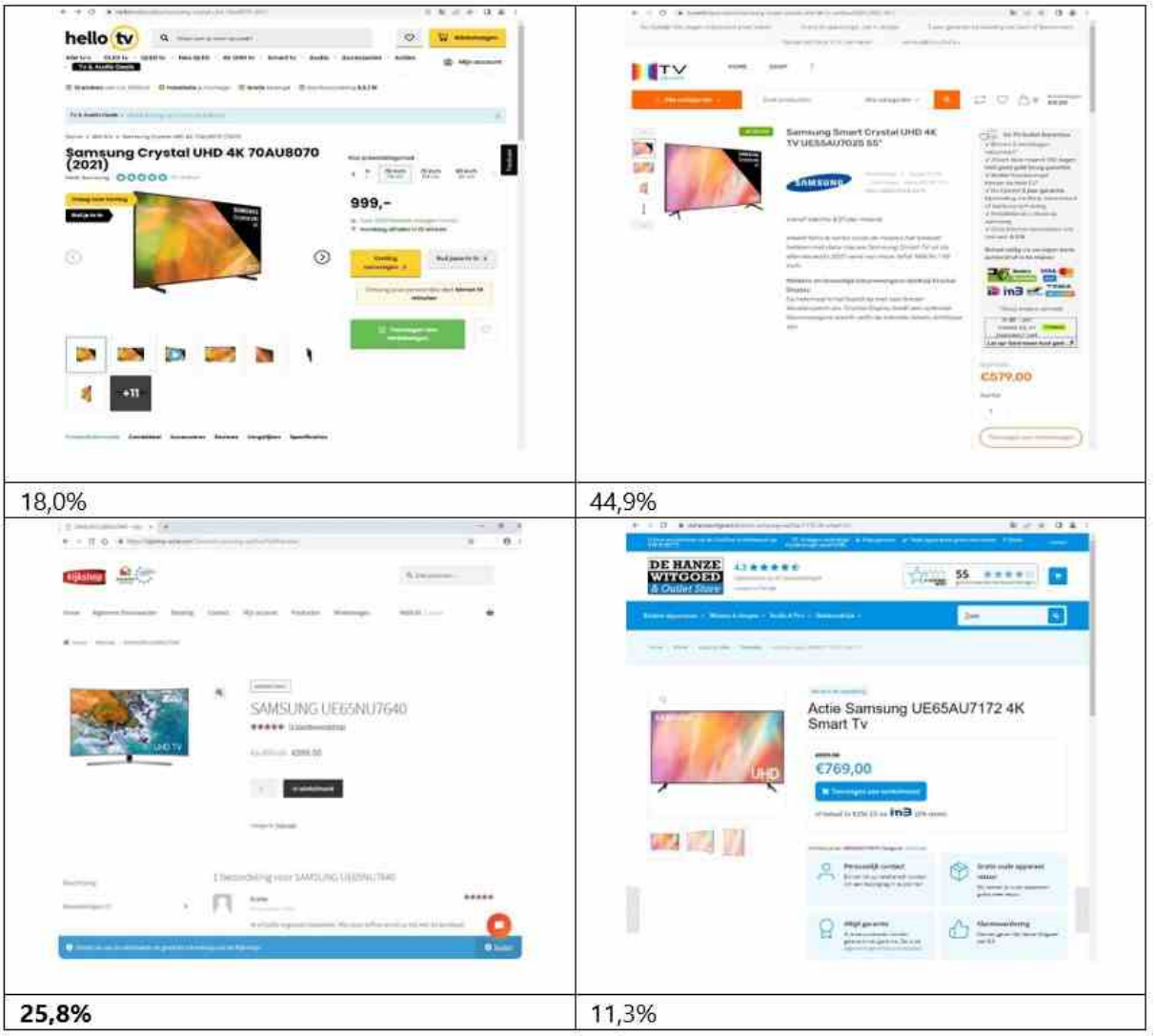
[16] n = 602.
[17] n = 81.
[18] We schatten hiervoor een model waarbij we knoppenkennis, privacy attitude, inschatting eigen digitale vaardigheden, de kritische digitale vaardigheden (informatie, communicatie, content), angst, schaamte en persoonskenmerken (geslacht, leeftijd, opleidingsniveau, stedelijkheid, regio, migratieachtergrond, religie, of men thuis een andere taal spreekt, of men ZZP'er is, of men wel of niet werkt of studeert en of men wel of geen partner heeft) schatten op het correct uitvoeren van de taak. We beschrijven alleen de factoren die een significante invloed hebben op het wel of niet correct uitvoeren van de taak. Voor degenen die een of beide antwoorden niet konden vinden werd het antwoord gecodeerd als incorrect. N = 680.
[19] Opleidingsniveau laag: p = 0,005.
[20] Kritische content vaardigheden: p < 0,001.
[21] Stedelijkheid: p = 0,010.
[22] Migratieachtergrond: p = 0,015.
[23] Link naar website van de consumentenbond. Meeliftend op de naam van het failliete Kijkshop openden criminelen een webshop op kijkshop-actie.com. Het aanbod varieerde van luxeproducten, zoals tablets en tv's, tot enkele populaire goedkopere artikelen, zoals een Senseo. Om vertrouwen te wekken hadden sommige producten positieve gebruikersreviews. De site heeft meerdere weken online gestaan.
[24] n = 689.
[25] n = 523, hierbij zijn respondenten die "weet ik niet" als antwoord gaven niet meegenomen.

nepwebwinkel werd dus niet zo vaak herkend als niet betrouwbaar. Toch **dacht 72,8% het goede antwoord** gegeven te hebben.[26] Deze taak werd door 50,7% van de respondenten als **best wel of heel moeilijk** bevonden.[27] Het merendeel heeft de websites **niet nagezocht** (89,1%).[28]

Meer dan de helft van de respondenten denkt te **weten op welke kenmerken ze moeten letten** om te beoordelen of een webwinkel betrouwbaar is (53,8%), ook heeft meer dan de helft er **vertrouwen in dat zij een nepwebwinkel kunnen herkennen** (54,3%). Toch denkt 31,8% **risico te lopen om slachtoffer te worden** van een aankoop bij een nepwebwinkel, zie figuur 3.4.[29]

Mensen denken dus dat ze een nepwebwinkel kunnen herkennen, zoeken niet na of een website echt onbetrouwbaar is, maar weten vervolgens de nepwebwinkel niet te herkennen als minst betrouwbaar. Wat hierbij wel meegespeeld heeft is dat dit voor respondenten best een lastige opdracht was.

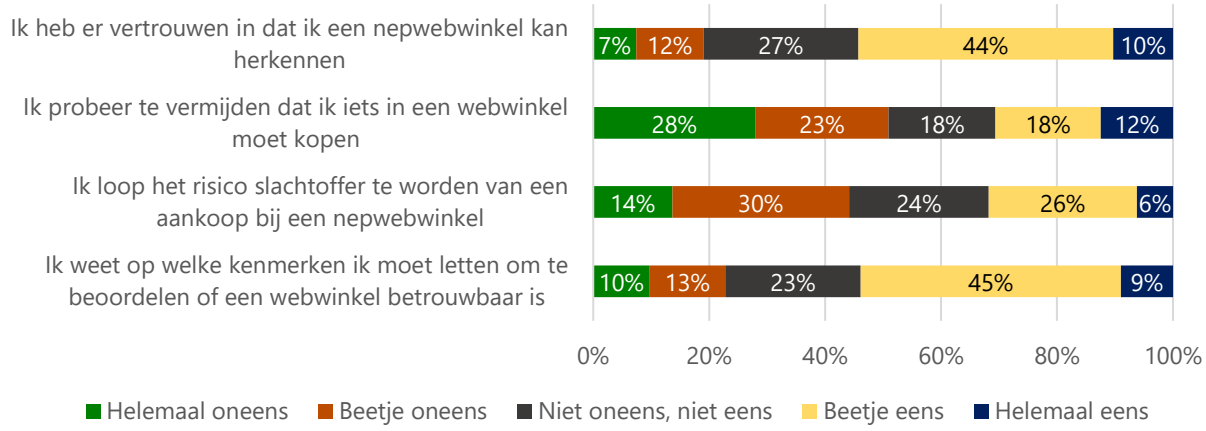
Figuur 3.3 Herkennen van de nepwebshop.



18,0%	44,9%
25,8%	11,3%

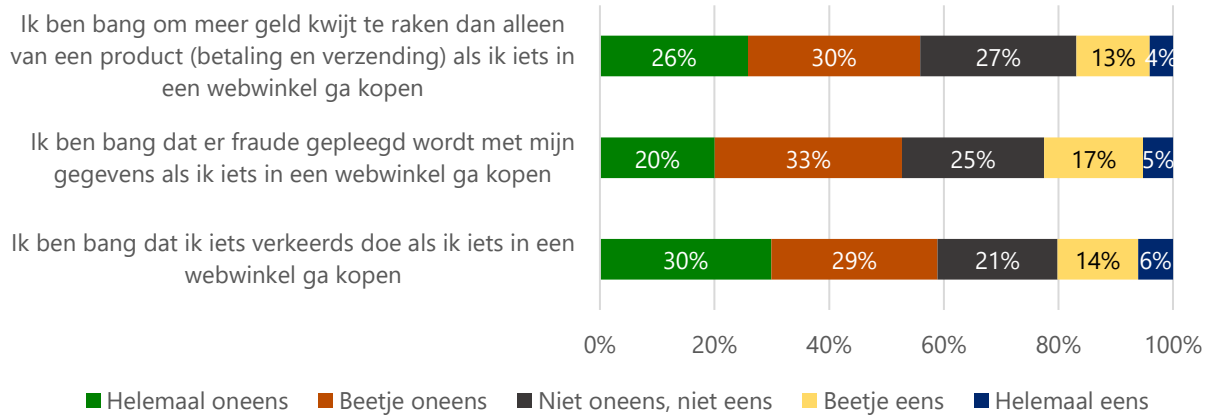
[26] *n* = 523.
[27] *n* = 523.
[28] *n* = 523.
[29] Het gaat hier om helemaal eens en een beetje eens bij elkaar opgeteld, voor *n* = 689.

Figuur 3.4 Herkennen nepwebwinkel



Verder blijkt dat 20,2% van de respondenten **bang is om iets verkeerd te doen als ze iets in een webwinkel gaan kopen**, dat 22,5% van de respondenten **bang is dat er fraude gepleegd wordt** met gegevens en dat 16,8% **bang is om meer geld kwijt te raken** dan alleen van het product (de betaling + verzending; zie ook figuur 3.5).[30]

Figuur 3.5 Aankopen in webwinkel



Tot slot blijkt dat **vrouwen** meer moeite hebben met het herkennen van de nepwebwinkel.[31] Namelijk 22,8% van de vrouwen gaf het goede antwoord vergeleken met 28,6% van de mannen.[32] Ook zien we dat de **leeftijd** een rol speelt.[33] Met name jongeren (16-24 jaar) zijn beter in het herkennen van de nepwebwinkel (40,9%) ten opzichte van mensen ouder dan 55+, die hier minder goed in zijn (55-64 jaar: 18,3% en 65+: 16,1%).[34]

[30] Het gaat hier om helemaal eens en een beetje eens bij elkaar opgeteld, voor n = 689.
[31] We schatten hiervoor een model waarbij we knoppenkennis, privacy attitude, inschatting eigen digitale vaardigheden, de kritische digitale vaardigheden (informatie, communicatie, content), angst, schaamte en persoonskenmerken (geslacht, leeftijd, opleidingsniveau, stedelijkheid, regio, migratieachtergrond, religie, of men thuis een andere taal spreekt, of men ZZP'er is, of men wel of niet werkt of studeert en of men wel of geen partner heeft) schatten op het correct uitvoeren van de taak. We beschrijven alleen de factoren die een significante invloed hebben op het wel of niet correct uitvoeren van de taak. Hierbij zijn respondenten die "weet ik niet" antwoorden niet meegenomen in de analyse. n = 523.
[32] Geslacht: p = 0,032.
[33] Leeftijd: p = 0,003.
[34] p = 0,035 en p = 0,006; de andere leeftijdscategorieën verschilden niet significant van elkaar.

Herkennen van nepnieuws

Respondenten kregen drie nieuwsberichten te zien, waarvan twee nepnieuwsberichten en moesten aangeven hoe betrouwbaar zij dachten dat het bericht leek (van 0 tot 100, waarbij 0 helemaal niet betrouwbaar was en 100 zeker wel betrouwbaar).

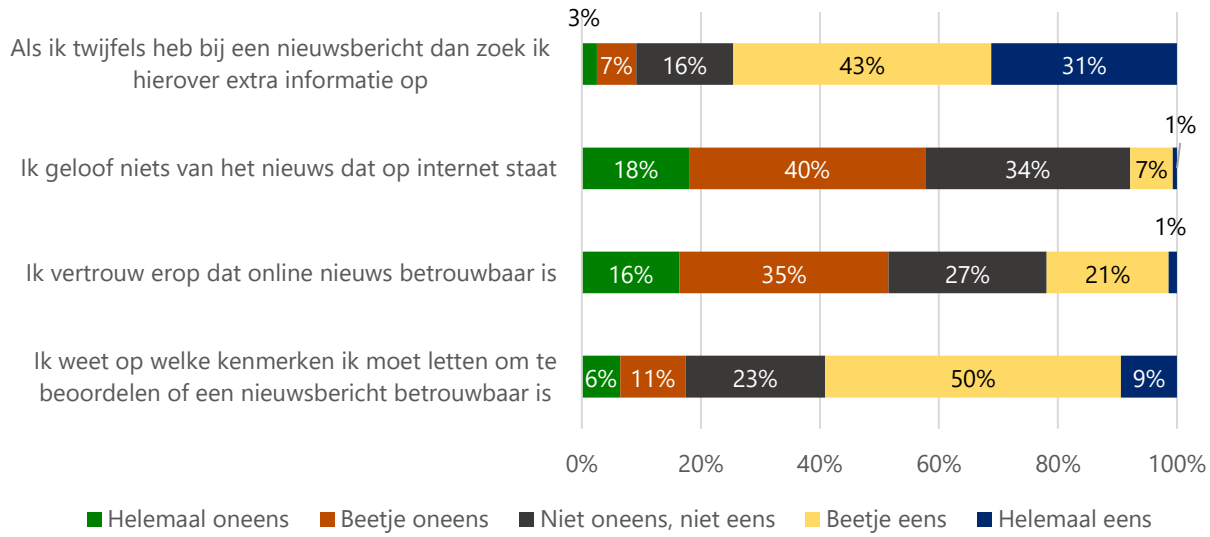
Figuur 3.6 Waargenomen betrouwbaarheid berichten

De waargenomen betrouwbaarheid was 24,2 en 54,8 voor de nepnieuwsberichten en 76,5 voor het echte bericht, wat aangeeft dat respondenten over het algemeen **onderscheid konden maken tussen deze verschillende soorten berichten**, zie ook figuur 3.6.[35] Wel wordt het eerste nepnieuwsbericht – de NOS berichtgeving over Ali B – duidelijk beter herkend als nepnieuws dan het nepnieuwsbericht van RTV Utrecht over het anti-autobrandsysteem, waar wat meer twijfel over is. Een groot deel van de respondenten was ervan overtuigd alle vragen goed te hebben (41,6%) of twee van de drie vragen (39,2%). 24,3% van de respondenten vond het een (heel) moeilijke taak.

[35] *n* = 712.

Meer dan de helft van de respondenten denkt te weten op welke kenmerken ze moeten letten om te beoordelen of een nieuwbericht betrouwbaar is (59,1%). Ongeveer een vijfde van de respondenten vertrouwt erop dat het online nieuws betrouwbaar is en 7,9% van de respondenten gelooft niets van het nieuws dat op internet staat. Driekwart van de respondenten trekt bij twijfel het nieuwsbericht na (74,6%), zie ook figuur 3.7.[36]

Figuur 3.7. Herkennen van nepnieuws



Tot slot blijkt dat **leeftijd** een rol speelt bij het kunnen herkennen van een nepwebwinkel.[37] Met name ouderen (65+) zijn beter in het herkennen van nepnieuws (52,6%).[38] 35-44'ers zijn hier het slechtst in (17,1%).[39] Ook **opleidingsniveau** speelt een rol, mensen met alleen basisonderwijs of vmbo niveau zijn slechter in het herkennen van nepnieuws (26,2% vs. gemiddeld 36,0% voor de andere opleidingsniveaus).[40]

Herkennen van phishing

Respondenten kregen drie berichten te zien, waarvan twee phishing berichten. Om de gevoeligheid voor phishing zowel cognitief als gedragsmatig vast te stellen beoordeelden respondenten in hoeverre het bericht spam leek (van 0 tot 100, waarbij 0 het bericht is zeker geen spam en 100 het bericht is zeker wel spam was) en welk gedrag ze zouden kiezen (de gevraagde actie uitvoeren, bericht bewaren, bericht weggooien, meer informatie zoeken, een melding maken). Op deze manier kunnen drie maten voor gevoeligheid voor phishing berekend worden:[41]

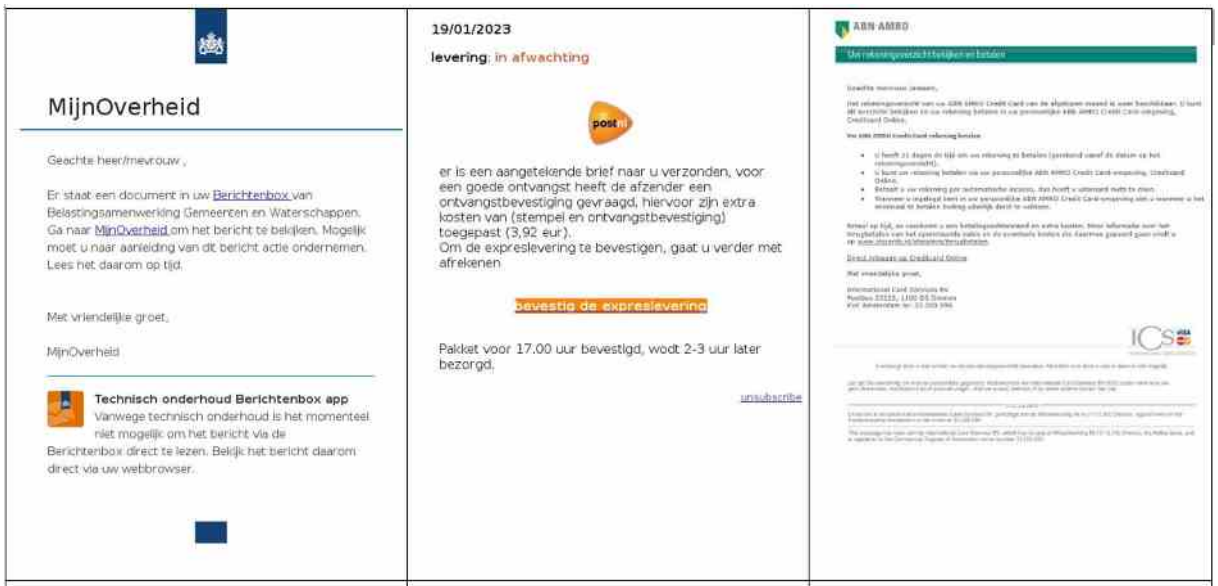
[36] Het gaat hier om helemaal eens en een beetje eens bij elkaar opgeteld.
[37] Leeftijd: p = 0,005.
[38] 65+: significant verschillend van alle leeftijdscategorieën behalve 55-64 jaar, alle p 's < 0.05.
[39] 35-44 jaar: significant verschillend van 55-64 jaar (p = 0,010) en 65+ (p < 0,001).
[40] Opleiding: p = 0,031.
[41] Zie ook: Kleitman, S., Law, M. K., & Kay, J. (2018). It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PloS one*, 13(10), e0205089.

- gemiddelde percepties van in hoeverre een bericht spam is (voor phishing berichten en echte (niet-phishing) berichten);
- frequenties van de gedragingen;
- nauwkeurigheid van detectie.[42]

De nauwkeurigheid van de detectie van phishing berichten was 69,8% (MijnOverheid) en 92,2% (PostNL).[43] Dit betekent dat respondenten over het algemeen 30,2% (MijnOverheid) en 7,8% (PostNL) van de phishing berichten bewaarden of de gevraagde actie uit zouden voeren. De detectienauwkeurigheid voor het legitieme bericht was 58,0%, wat betekent dat 42,0% het legitieme bericht (onterecht) zou weggooien of hier melding van zou maken. De waargenomen perceptie van of het bericht spam is, was 62,2 voor het eerste phishing bericht (van MijnOverheid) en 86,9 voor het tweede phishing bericht (van PostNL) en het was 53,9 voor het legitieme bericht (van ABN-AMRO/ICS), wat aangeeft dat respondenten **niet zo goed onderscheid konden maken tussen deze verschillende soorten berichten**, zie figuur 3.8. Voor het PostNL bericht lukt dit wel goed, maar de berichten van de overheid of creditcard worden vaker foutief gedetecteerd. Kanttekening hier is dat men beter té voorzichtig kan zijn en er dus ook wat voor te zeggen valt om geen gevolg te geven aan het legitieme bericht. Alhoewel dit ook aangeeft dat men het lastig vindt om te beoordelen of iets nu goed of fout en (on)betrouwbaar is.

Deze taak werd door 30,4% van de respondenten als (best wel) **moeilijk** bevonden. Een groot deel van de respondenten was ervan overtuigd alle vragen goed te hebben (41,3%) of twee van de drie vragen goed te hebben (44,6%).

Figuur 3.8. Waargenomen percepties of berichten spam zijn (gemiddelde op een schaal van 0-100)

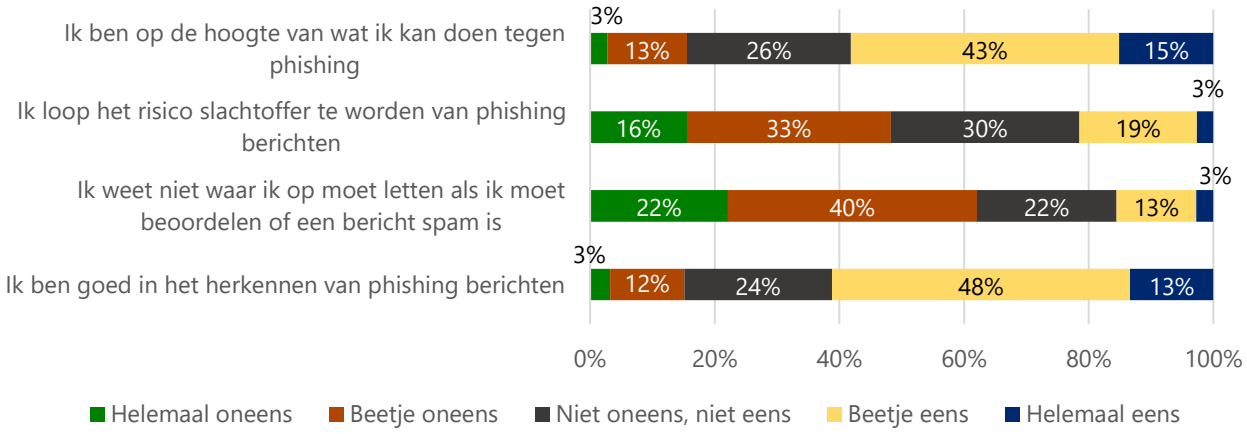


[42] De nauwkeurigheid van detectie werd gecodeerd, waarbij de juiste antwoorden zijn "weggooien" of "meer informatie zoeken" voor phishingberichten; en "het bewaren" of "zoeken van meer informatie" voor echte berichten. Het "zoeken naar meer informatie" werd dus als correct gecodeerd voor zowel phishing als echte berichten omdat dit juist gedrag is in beide situaties. Het kan voorkomen dat respondenten een echt bericht voor phishing aanmerken (weg gooien), dat wordt dus gerekend als niet nauwkeurig.

[43] n = 688.

Meer dan de helft van de respondenten denkt phishing goed te kunnen **herkennen** (61,2%) en geeft aan op de hoogte te zijn van **wat te doen tegen phishing** (58,1%).[44] Ongeveer een vijfde van de respondenten denkt **risico te lopen om slachtoffer te worden** van phishing berichten (21,5%) en zo'n 15,6% **weet niet waar op te letten** als ze moeten beoordelen of een bericht kwaadaardig is, zie ook figuur 3.9.

Figuur 3.9 Herkennen van phishing berichten



Het blijkt dat **vrouwen** beter zijn in het herkennen van phishing berichten.[45] Namelijk 40,7% van de vrouwen gaf het goede antwoord vergeleken met 32,4% van de mannen.[46] Opvallend is verder dat leeftijd of opleidingsniveau geen rol speelt en dit dus een probleem van alle leeftijden en achtergronden is.[47] Wel blijkt dat **knoppenkennis**, **kritische informatievaardigheden** en **schaamte** een rol spelen.[48] Mensen die goed waren in het herkennen van phishing berichten hadden (iets) meer knoppenkennis (M = 4,95), (iets) meer kritische informatievaardigheden (M = 4,20) en ervaren minder schaamte (M = 1,44) dan mensen die de vragen fout hadden (knoppenkennis: M = 4,85; kritische informatievaardigheden: M = 4,19; schaamte M = 1,67). Tot slot blijkt dat mensen uit **West- en Oost-Nederland** (Oost: Overijssel, Gelderland, Flevoland; West: Noord-Holland, Zuid-Holland, Zeeland) iets beter zijn in het herkennen van phishing (37,8%) dan mensen uit Noord-Nederland (24,3%; Groningen, Friesland, Drenthe) en Zuid-Nederland (31,3%; Noord-Brabant, Limburg).[49]

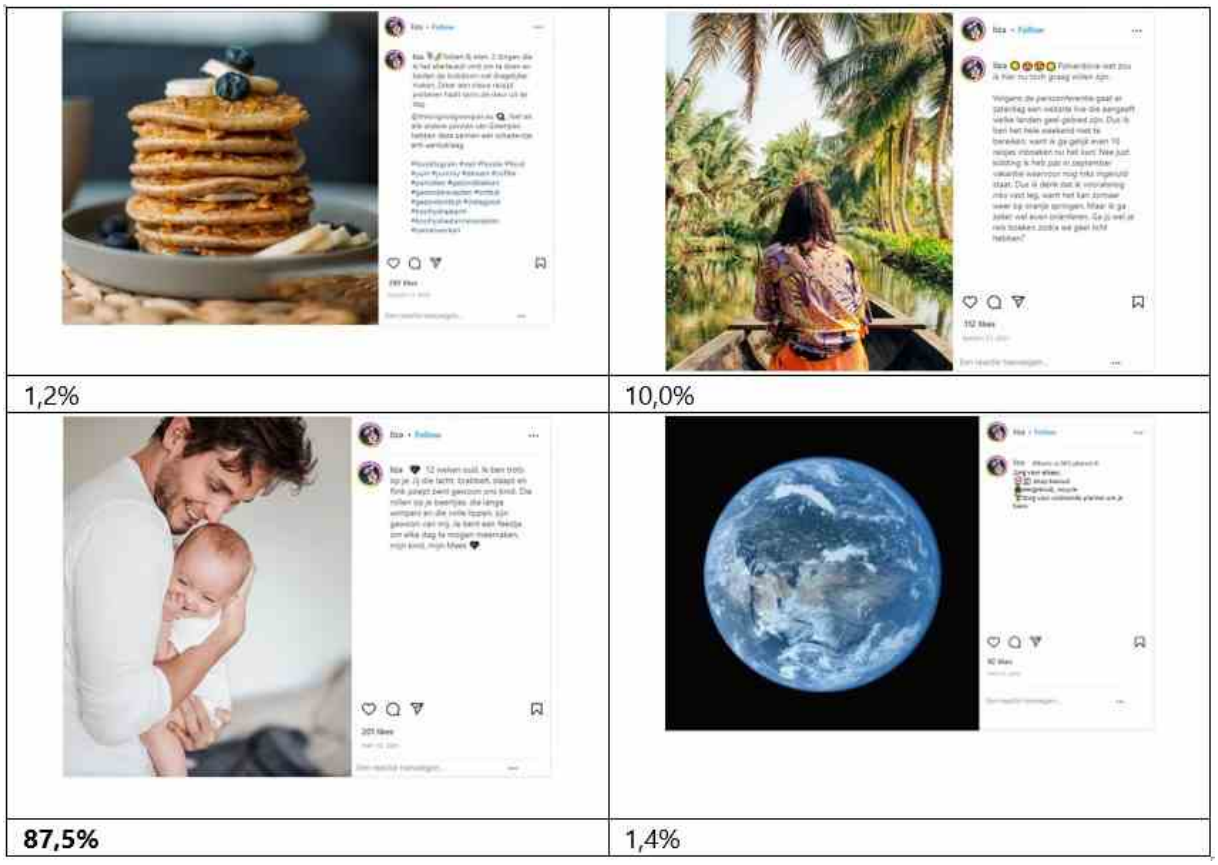
Adequaat gebruik van social media

Respondenten kregen vier social media berichten van Liza te zien. Ze werden gevraagd welk bericht zij zeker niet mogen delen met anderen zonder het aan Liza te vragen. Deze vraag werd alleen gesteld

[44] Het gaat hier om helemaal eens en een beetje eens bij elkaar opgeteld.
[45] We schatten hiervoor een model waarbij we knoppenkennis, privacy attitude, inschatting eigen digitale vaardigheden, de kritische digitale vaardigheden (informatie, communicatie, content), angst, schaamte en persoonskenmerken (geslacht, leeftijd, opleidingsniveau, stedelijkheid, regio, migratieachtergrond, religie, of men thuis een andere taal spreekt, of men ZZP'er is, of men wel of niet werkt of studeert en of men wel of geen partner heeft) schatten op het correct uitvoeren van de taak. We beschrijven alleen de factoren die een significante invloed hebben op het wel of niet correct uitvoeren van de taak. Omdat er drie keer een bericht beoordeeld werd is er een totaalscore berekend over deze berichten heen (waarbij alle drie de vragen dus goed beantwoord moesten zijn). n = 688.
[46] Geslacht: p = 0,045.
[47] alle p's > 0,05.
[48] Knoppenkennis: p = 0,014; kritische informatievaardigheden: p = 0,013; schaamte: p = 0,034.
[49] Noord vs. andere regio's: p = 0,013; Zuid vs. andere regio's: p = 0,027.

aan respondenten die gebruik maken van social media. 11,0% van de respondenten wist niet welk bericht zij niet zomaar mogen delen.[50] Als we deze groep niet meenemen dan bleek dat het merendeel van de respondenten (87,5%) wist **welk bericht men niet met anderen mag delen zonder het te vragen**, 12,5% wist dit niet, zie figuur 3.10.[51] 89,5% dacht het goede antwoord gegeven te hebben, dat komt dus redelijk overeen. Deze vraag werd door 15,7% van de respondenten als **best/heel moeilijk** gevonden.[52]

Figuur 3.10 Identificeren van het social media bericht dat men niet mag delen met anderen

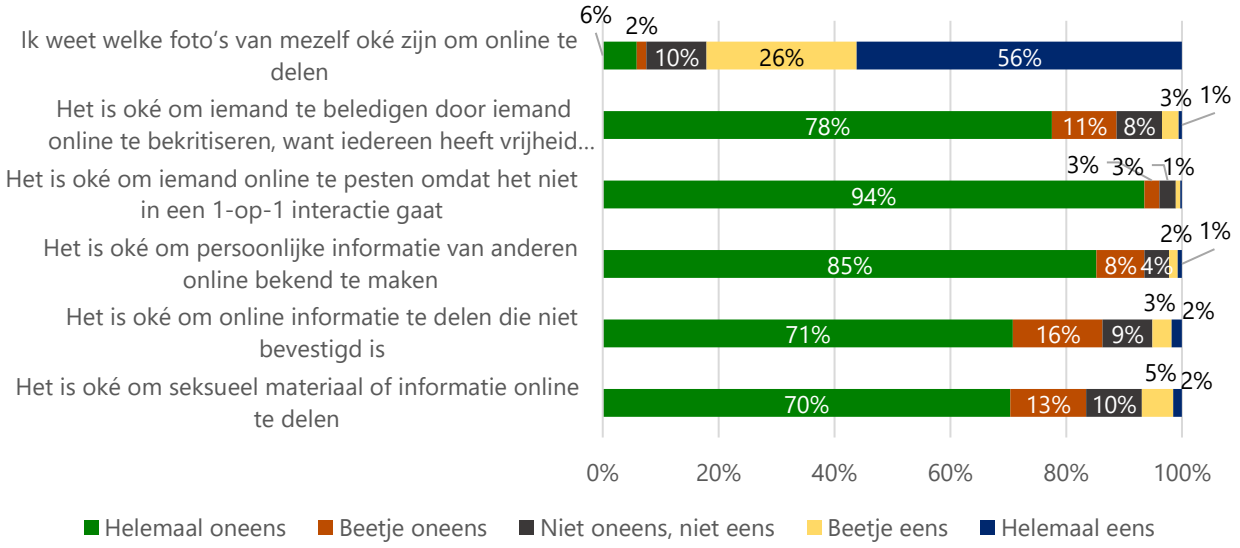


Alhoewel veel mensen wisten welk bericht ze niet met anderen mogen delen zonder het te vragen zijn er toch enkele verschillen.[53] Het blijkt dat leeftijd een rol speelt, met name **65+'ers zijn hier minder** goed in (78,1% correct vs. gemiddeld 89,7% correct voor de andere leeftijdscategorieën).[54] Ook weten **hoger opgeleiden** beter welk bericht ze niet zomaar met anderen mogen delen (92,2% vs. 82,8%).[55] Verder blijkt dat **knoppenkennis** een rol speelt.[56] Mensen die goed wisten welke berichten zij niet

[50] n = 664.
[51] n = 591.
[52] Door 21,4% als we ook de respondenten die "weet ik niet" antwoorden meenemen.
[53] We schatten hiervoor een model waarbij we knoppenkennis, privacy attitude, inschatting eigen digitale vaardigheden, de kritische digitale vaardigheden (informatie, communicatie, content), angst, schaamte en persoonskenmerken (geslacht, leeftijd, opleidingsniveau, stedelijkheid, regio, migratieachtergrond, religie, of men thuis een andere taal spreekt, of men ZZP'er is, of men wel of niet werkt of studeert en of men wel of geen partner heeft) schatten op het correct uitvoeren van de taak. We beschrijven alleen de factoren die een significante invloed hebben op het wel of niet correct uitvoeren van de taak. Hierbij zijn respondenten die "weet ik niet" antwoorden niet meegenomen in de analyse. n = 565.
[54] Leeftijd: p = 0,012; 65+ verschilde significant van de leeftijdscategorie 25-34 jaar (p = 0,001; 96,1% gaf het goede antwoord in deze leeftijdscategorie).
[55] Opleidingsniveau hoog: p = 0,003.
[56] Knoppenkennis: p = 0,012.

mogen delen hadden iets meer knoppenkennis (*M* = 4,93 vs. *M* = 4,76) en waren minder bezorgd over hun online **privacy** (*M* = 3,68 vs. *M* = 3,90).[57]
Verder geeft 82,1% van de respondenten aan **goed te weten welke foto's van zichzelf oké** zijn om online te delen.[58] Het merendeel vindt het **niet oké** om iemand **online te beledigen** (88,7%), om **seksueel materiaal of informatie online** te delen (83,4%), om informatie online te delen die **niet bevestigd** is (86,3%), om **persoonlijke informatie van anderen** online bekend te maken (93,5%), of **online te pesten** (96,1%), zie ook figuur 3.11. [59]

Figuur 3.11 Adequaat social media gebruik



Omgang met zoekresultaten en filterbubbel

In dit deel van de vragenlijst werd aan respondenten gevraagd hoe zij met gesponsorde zoekresultaten omgaan als ze een zoekmachine gebruiken. Meer dan de helft van de respondenten slaat de gesponsorde resultaten over (58,1%), 18,2% bekijkt bewust (ook) de gesponsorde resultaten en 23,7% let er niet op of de zoekresultaten gesponsord zijn of niet.

Vervolgens gaven we respondenten informatie over zoekmachines. We legden uit dat veel zoekmachines gegevens van iemand verzamelen. Deze gegevens worden gebruikt om beter te voorspellen waarnaar iemand precies op zoek is als deze een zoekopdracht geeft. Met de verzamelde gegevens worden de gewone en gesponsorde zoekresultaten op deze persoon afgestemd. Vervolgens gaven we een lijst van verschillende soorten gegevens die een zoekmachine van iemand zou kunnen verzamelen en gebruiken om zoekresultaten persoonlijk te maken. Respondenten moesten per soort aangeven wat zij ervan zouden vinden als een zoekmachine deze gegevens gebruikt.

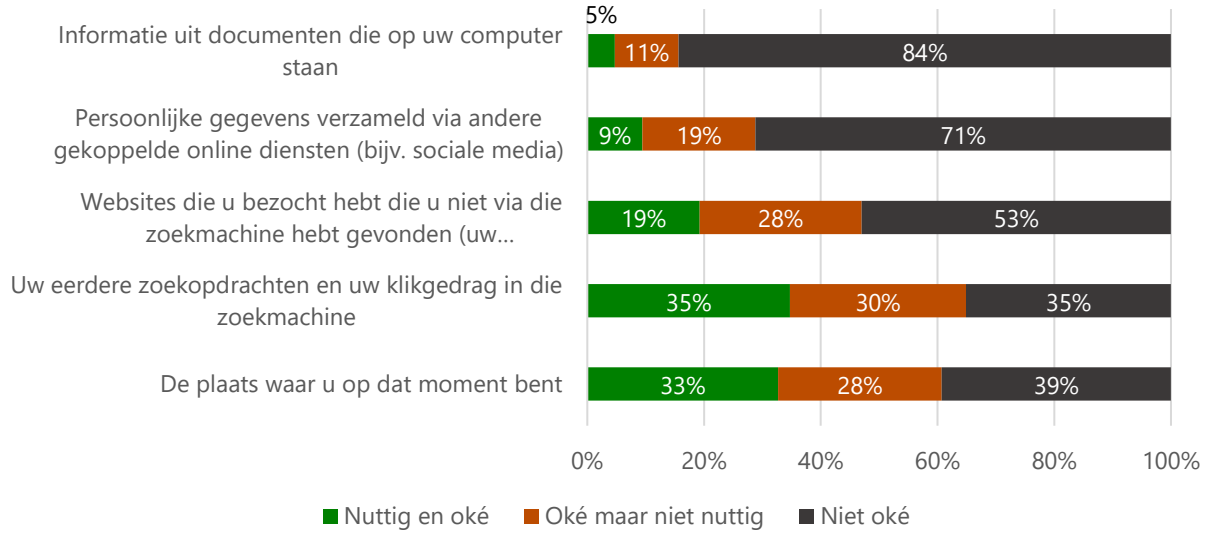
Ongeveer een derde van de respondenten vindt het nuttig en oké dat een zoekmachine persoonlijke zoekresultaten geeft op basis van de plaats waar iemand is (32,7%) en de eerdere zoekopdrachten (34,7%). Men vindt het niet oké als er informatie gebruikt wordt uit documenten op de computer

[57] Privacy attitude: p = 0,031.
[58] Het gaat hier om helemaal eens en een beetje eens bij elkaar opgeteld, voor n = 664.
[59] Het gaat hier om helemaal oneens en een beetje oneens bij elkaar opgeteld, voor n = 664.

(84,4%) of persoonlijke gegevens verzameld via andere gekoppelde online diensten zoals social media (71,2%), zie ook figuur 3.12.

Hoe bezorgder men is over de eigen privacy, hoe minder acceptabel men het gebruik van personalisering van gegevens vindt.[60] Verder blijkt dat mensen ouder dan 55 jaar het gebruik van de plaats waar zij op dat moment zijn en het gebruik van informatie uit eerdere zoekopdrachten minder oké vinden dan jongeren.[61] Waar 39,2% van de 16-24 jarigen het nuttig en oké vindt om gepersonaliseerde zoekresultaten op basis van locatie te krijgen, vindt slecht 19,6% van de 65+'ers dit en 24,8% van de 55-64-jarigen. Eenzelfde patroon zien we voor het gebruik van informatie uit eerdere zoekopdrachten: waar 59,8% van de 16-24 jarigen dit nuttig en oké vindt is dat slechts het geval voor 22,4% van de 55-64-jarigen en voor 20,3% van de 65+'ers.

Figuur 3.12 Personalisering van zoekresultaten



3.2.3 Bijscholing en digitale vaardigheden kinderen

Bijscholing

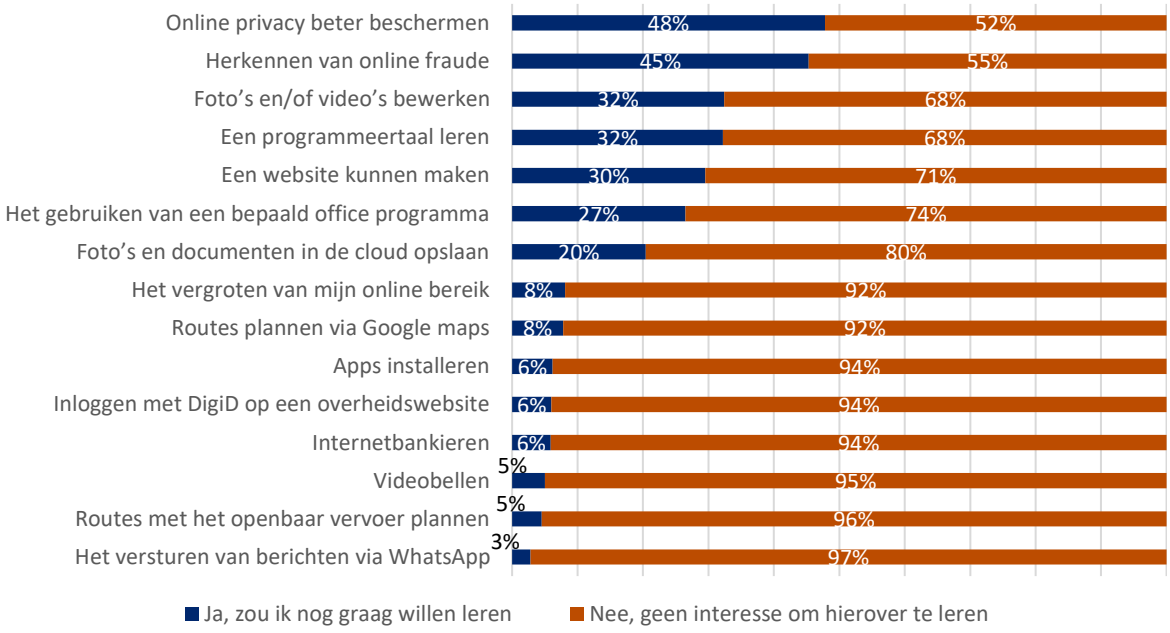
We onderzochten ook de leerbehoefte van respondenten. De meerderheid (70,5%) van alle respondenten gaf aan tenminste één ding te willen leren op het gebied van digitale vaardigheden. Deze **algemene leerbehoefte** van respondenten was afhankelijk van geslacht,[62] maar niet van

[60] We schatten hiervoor een model waarbij we knoppenkennis, privacy attitude, inschatting eigen digitale vaardigheden, de kritische digitale vaardigheden (informatie, communicatie, content), angst, schaamte en persoonskenmerken (geslacht, leeftijd, opleidingsniveau, stedelijkheid, regio, migratieachtergrond, religie, of men thuis een andere taal spreekt, of men ZZP'er is, of men wel of niet werkt of studeert en of men wel of geen partner heeft) schatten op de gegeven antwoorden (multinomiale regressie). Voor alle typen gegevensgebruik: p <0,05. Daarnaast zijn er nog enkele andere significante effecten die hier niet gerapporteerd worden.
[61] Locatiegegevens: p < 0,001; informatie uit eerdere zoekopdrachten: p < 0,001.
[62] p < 0,001.

leeftijd.[63] Vrouwen gaven vaker aan ten minste een ding te willen leren (74,9%) dan mannen dat deden (66,3%), maar tussen de verschillende leeftijdsgroepen was geen verschil op algemene leerbehoeften.

Van alle respondenten met een leerbehoefte gaf een groot deel aan te willen leren hoe ze hun online privacy beter kunnen beschermen (47,8%) en hoe ze online fraude kunnen herkennen (45,3%), zie figuur 3.13. Daarnaast gaven respondenten aan dat zij ook graag de meer praktische vaardigheden wilden leren, bijvoorbeeld het bewerken van foto's en/of video's (32,4%), het gebruik van een bepaalde programmeertaal (32,2%) en het maken van een website (29,5%). Ook andere digitale vaardigheden, zoals het leren van een bepaald office programma (26,5%) en opslaan van foto's en documenten in de cloud (20,4%) werden vaak genoemd.

Figuur 3.13 Algemene leerbehoefte



De **specifieke leerbehoefte** verschilde iets per leeftijd en geslacht. Mannen wilden bijvoorbeeld liever een programmeertaal leren dan vrouwen (36,0% vs. 28,7%).[64] Vrouwen gaven daarentegen vaker aan te willen leren hoe ze hun online privacy beter kunnen beschermen (52,7% vs. 42,6% van de mannen).[65] Ook wilde 49,3% van de vrouwen meer leren over het herkennen van online fraude (vs. 40,9% van de mannen).[66]

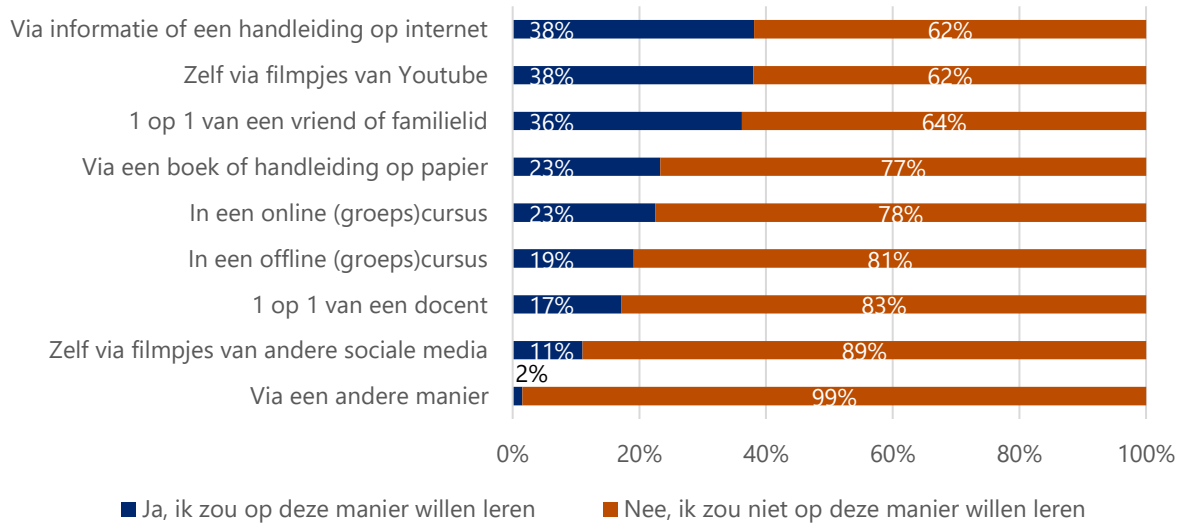
De leerbehoeften verschilden ook per leeftijdscategorie. Over het algemeen gaven jongeren vaker aan een programmeertaal te willen leren en was voor mensen van 35 jaar en ouder het herkennen van online fraude belangrijker. Hieronder geven we de top 3 per leeftijdscategorie:

- **16 – 24 jarigen:** (1) Leren van een programmeertaal (51,6%), (2) Online privacy beter beschermen (44,4%), (3) Website maken (40,6%).
- **25 - 34 jarigen:** (1) Leren van een programmeertaal (48,4%), (2) Online privacy beter beschermen (42,9%), (3) Website maken (32,9%).

[63] $p = 0{,}293$.
[64] $p < 0{,}005$.
[65] $p < 0.01$.
[66] $p < 0{,}010$.

- **35 - 44 jarigen:** (1) Online privacy beter beschermen (49,9%), (2) Leren van een programmeertaal (42,9%), (3) Herkennen van fraude (39,9%).
- **45 - 54 jarigen:** (1) Herkennen van online fraude (51,9%), (2) Online privacy beter beschermen (51,2%), (3) Website maken (40,6%).
- **55 - 64 jarigen:** (1) Herkennen van online fraude (51,9%), (2) Online privacy beter beschermen (43,6%), (3) Foto's en video's bewerken (36,8%).
- **65+'ers:** (1) Herkennen van online fraude (59,0%), (2) Online privacy beter beschermen (49,8%), (3) Foto's en video's bewerken (36,4%).

Tot slot gaven de meeste respondenten de voorkeur aan leren via een handleiding op internet (38,1%), via filmpjes van Youtube (38,0%), of via 1 op 1 leren van vriend of familielid (36,2%, zie figuur 3.14).



Figuur 3.14. Manier van leren

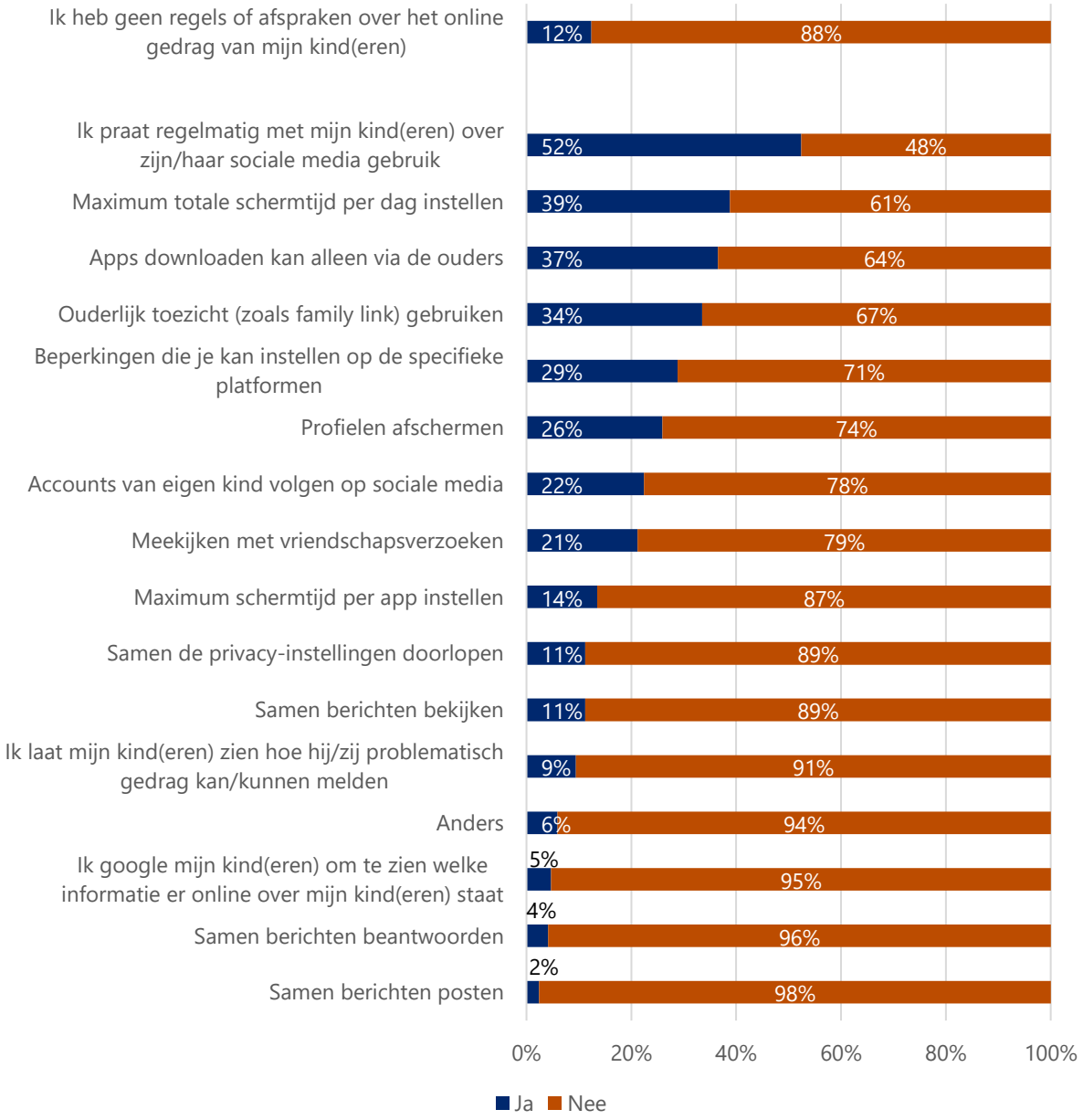
Digitale vaardigheden kinderen

Aan respondenten met thuiswonende kinderen in de leeftijd van 7 tot 15 jaar, vroegen we welke **sociale media hun kinderen** gebruiken en welke afspraken gemaakt zijn over het online gedrag van de kind(eren).[67] 91,8% van de ouders gaf aan dat hun kinderen een of meerdere sociale media gebruiken. De meest gebruikte sociale media onder kinderen in de leeftijd 7 – 15 jaar waren YouTube (76,5%), Whatsapp (66,5%), TikTok (52,9%), Snapchat (46,5%) en Instagram (40%).

Ruim 12% van de ouders gaf aan dat ze **geen regels of afspraken** hebben met hun kinderen over het online gedrag. Van de bijna 88% van de ouders die wel afspraken met hun kinderen maakten over het online gedrag gaf meer dan de helft aan regelmatig met hun kinderen te praten over hun gedrag online, zie figuur 3.15. Een groot deel van de ouders heeft ook een maximum schermtijd per dag ingesteld (38,8%). 36,5% van de ouders geeft aan dat kinderen alleen apps via de ouders kunnen downloaden en 33,5% van de ouders gebruikt een applicatie voor ouderlijk toezicht (zoals family link) op de smartphone van hun kinderen.

[67] *n* = 170.

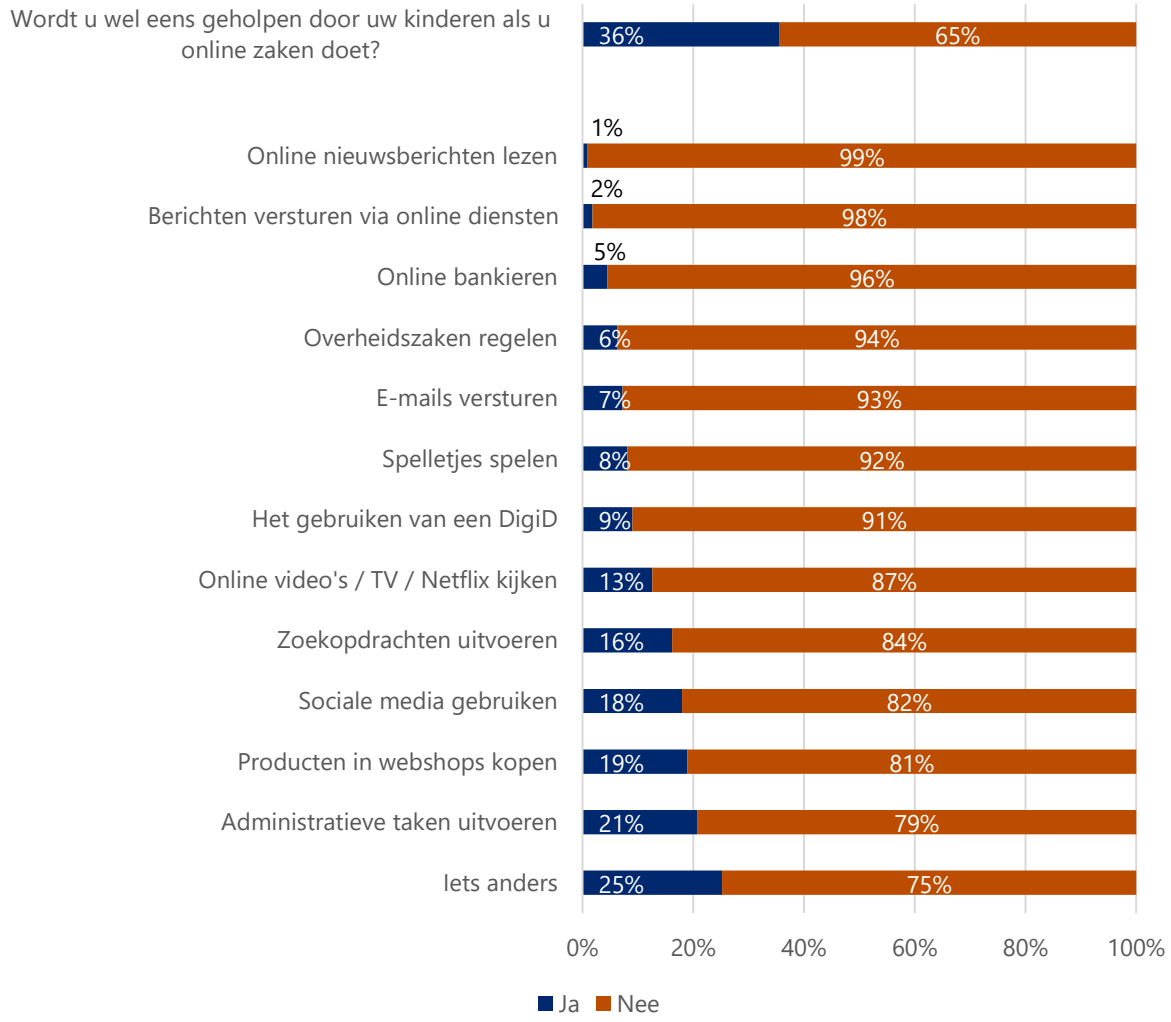
Figuur 3.15 Afspraken rondom online gedrag kinderen



Ook vroegen we respondenten met kinderen van 7 jaar of ouder of en waarmee men zelf wel eens geholpen werd door hun kinderen met online zaken, zie figuur 3.16. 35,5% van alle ouders werd wel eens door hun kinderen hiermee geholpen. 20,7% van de respondenten werden voornamelijk door hun kinderen geholpen met administratieve taken uitvoeren (bijvoorbeeld formulieren invullen, loonstroken downloaden of een declaratie invullen) en 18,9% werd ook wel eens geholpen wanneer ze online producten wilden kopen.

Ruim 25% van de respondenten gaf aan dat ze wel eens met iets anders werden geholpen dan de opties waaruit gekozen kon worden. Uit de open antwoorden bleek het te gaan om bijvoorbeeld het bewerken van foto's, het herkennen van spam mail, internet en pc problemen oplossen en het overzetten van bestanden naar een nieuwe telefoon of laptop.

Figuur 3.16 Hulp van eigen kinderen bij online zaken



3.3 Conclusies en aanbevelingen voor fase 3

Op basis van het vragenlijstonderzoek blijken voor een aanzienlijk deel van de mensen twee situaties problematisch te zijn: (1) Het herkennen van een nepwebwinkel en (2) het herkennen van phishing mails. Deze problemen staan daarom dan ook centraal in fase 3.

Uit de vragenlijst bleek dat mensen denken dat ze een nepwebwinkel kunnen herkennen, maar dat ze niet goed nazoeken of een website echt onbetrouwbaar is en dat ze vervolgens de nepwebwinkel niet goed weten te herkennen. Wat hierbij wel meegespeeld heeft is dat dit voor respondenten best een lastige opdracht was. Met name vrouwen en ouderen (65+) hebben meer moeite met het herkennen van de nepwebwinkel. Ook leeft er onder bijna een derde van de respondenten de angst om slachtoffer te worden van een aankoop bij een nepwebwinkel. En is er bij zo'n 20% van de respondenten angst voor fraude met gegevens en angst om meer geld kwijt te raken bij een online aankoop. Webshopfraude komt steeds vaker voor en is een serieus probleem, zowel op persoonlijk vlak als voor de economie en samenleving. In 2021 is 17 procent van de bevolking, bijna 2,5 miljoen mensen, slachtoffer geweest van een of meer online delicten of incidenten. Tien procent (anderhalf

miljoen mensen) was slachtoffer van online oplichting en fraude.[68] Ook blijkt dat van de mensen die opgelicht zijn bij een online aankoop slechts 1 op de 10 mensen de schade vergoed kreeg.[69] De politie ontving in 2022 10.500 aangiften over fraude via nepwebshops. Het gemiddelde schadebedrag van gedupeerde klanten bedraagt €357. Het totale schadebedrag over 2022, was vóór de feestdagen al €3.731.486. Vermoedelijk ligt het schadebedrag nog hoger omdat niet iedereen aangifte doet.[70] Het is dus belangrijk om hier meer bewustwording op te creëren. In de verdiepende fase wordt daarom verder in gegaan op het volgende vraagstuk: Hoe kunnen we nog beter bewustwording creëren rondom het beoordelen van de betrouwbaarheid van webwinkels? En, specifiek voor kwetsbare groepen (bijvoorbeeld vrouwen en 65+'ers)?

Uit de vragenlijst bleek ook dat mensen niet zo goed onderscheid weten te maken tussen verschillende soorten berichten (wel of geen phishing). Dat dit ook een serieus individueel als economisch/financieel probleem is blijkt uit het feit dat in 2021 ruim honderdduizend personen zijn gedupeerd door phishing.[71] Het blijkt dat vaardigheden rondom het herkennen van phishing nog wel wat vergroot kunnen worden. Uit de vraag naar bijscholing blijkt dit namelijk een van de belangrijkste thema's te zijn (herkennen online fraude en beschermen online privacy). Verder blijkt dat mannen minder goed zijn in het herkennen van phishing berichten. Opvallend is verder dat leeftijd of opleidingsniveau geen rol speelt en dit dus een probleem van alle leeftijden en achtergronden lijkt te zijn. Wel blijkt dat mensen die goed waren in het herkennen van phishing berichten meer knoppenkennis hebben en (iets) meer kritische informatievaardigheden en dat zij minder schaamte ervaren (omtrent dingen die zij digitaal niet goed kunnen). Omdat dit probleem speelt bij alle leeftijden en achtergronden wordt er in de verdiepende fase verder in gegaan op het volgende vraagstuk: Hoe kunnen we nog beter bewustwording creëren rondom het herkennen van phishing? En, specifiek voor kwetsbare groepen (bijvoorbeeld mannen en mensen die geen hulp durven vragen omdat zij zich hiervoor schamen)?

[68] Link naar website CBS
[69] Cijfers uit 2018
[70] Link naar website van de politie
[71] Link naar website CBS

4 Fase 3: duiding en oplossingsrichtingen

De tweede focusgroep werd ná de kwantitatieve fase gehouden en was gericht op het duiden van de resultaten uit het vragenlijstonderzoek en het verzamelen van input over mogelijk kansrijke (voornamelijk informele) interventies. Dit deden we aan de hand van design thinking methodieken (zie Box 4.1).

Box 4.1 Uitleg design thinking

Met behulp van **design thinking** worden op een creatieve wijze innovatieve oplossingen bedacht. Dit wordt gedaan middels een brede brainstorm naar oplossingen op basis van de geïdentificeerde problemen en het inbeelden in de problematische situaties.

Design thinking is een ontwerpmethode waar in stappen naar één of meerdere oplossingen voor een maatschappelijk vraagstuk toe gewerkt wordt. Daarbij staat de mens centraal; de ervaringen en behoeften van de doelgroep zijn cruciaal bij het ontwikkelen van een oplossing. Design thinking bestaat uit vijf stappen. In de focusgroep is naar stap 3 toe gewerkt.

1. **Inleven**. Hierbij gaat het om het inleven vanuit het perspectief van de doelgroep. Zonder empathie, en dus zonder te weten wat er omgaat in anderen (gevoelens, gedachten, etc.) loop je het risico iets te ontwikkelen dat helemaal niet aansluit bij wat mensen nodig hebben. Op basis van de kwantitatieve fase (en eerdere inzichten uit de kwalitatieve fase) is bekend wat de meest voorkomende uitdagingen zijn. In de focusgroep wordt hier de nadruk op gelegd. Vervolgens moesten de experts zich inleven in wat iemand in deze situatie voelt en denkt.
2. **Definiëren**. Op basis van het inleven wordt het probleem verder geconcretiseerd en staat de doelgroep wederom centraal.
3. **Verbeelden**. In deze fase worden zoveel mogelijk oplossingen gegeneerd voor het probleem. Het gaat hierbij niet om het vinden van de perfecte oplossing, maar om zoveel mogelijk verschillende oplossingsrichtingen te bedenken.
4. **Prototype**. Hier gaat het om het creëren van een eerste versie van de oplossing, die past bij de doelgroep/eindgebruiker. Deze stap is geen onderdeel van de focusgroep.
5. **Testen en optimaliseren**. In deze fase wordt getest hoe de doelgroep de gekozen oplossing ervaart, wat werkt wel en wat werkt niet? Vervolgens wordt dit geoptimaliseerd. Deze stap is geen onderdeel van de focusgroep.

4.1 Methode

We waren te gast in De Koninklijke Bibliotheek en in een sessie van 2 uur is met 9 experts gesproken, van de Koninklijke Bibliotheek, Alliantie Digitaal Samenleven, het ECP, Netwerk Mediawijsheid, Seniorweb, Het Nationaal Ouderenfonds en Digisterker. De deelnemers kregen een vergoeding van €25 voor deelname. De experts hebben te maken met verschillende doelgroepen, variërend van mensen met een kleine portemonnee, mensen met een migratieachtergrond, en variërend van jong tot oud.

Discussies werden afgewisseld met opdrachten (met behulp van design thinking methodieken). Voor het inleven in verschillende groepen werd gewerkt met een *empathy map*. Een empathy map is een visualisatie van gedachtes, gevoelens, en gedragingen van een bepaalde doelgroep en wordt gebruikt voor het inleven in de wereld van deze doelgroep. Deze basis is nodig voor het komen tot oplossingen.

Voor het genereren van oplossingen werd gewerkt met de *wishful thinking methode*. Dit is een methode om de ideale situatie te beschrijven voor de verschillende (kwetsbare) groepen. Hieruit destilleren we bruikbare punten die we mee kunnen nemen naar de "echte" wereld. Middels een brede

brainstorm wordt zo gewerkt naar oplossingen op basis van de geïdentificeerde problemen en het inbeelden in de problematische situaties.

De gesprekshandleiding van de focusgroep is te vinden in Bijlage G.

4.2 Innovatieve oplossingen met design thinking

Op basis van de uitkomsten uit het vragenlijstonderzoek en de grote impact die deze fenomenen hebben op zowel individuen als de samenleving zijn twee problematische situaties gekozen die in de focusgroep centraal stonden: (1) Het herkennen van een nepwebwinkel en (2) De problemen rondom phishing mails.

4.2.1 Casus 1 – nepwebwinkels

Uit de afgenomen vragenlijst bleek dat mensen denken dat ze een nepwebwinkel kunnen herkennen, maar dat ze niet goed nazoeken of een website echt (on)betrouwbaar is en dat ze vervolgens de nepwebwinkel niet goed weten te herkennen. Vrouwen en ouderen (65+) bleken in het vragenlijstonderzoek minder goed te zijn in het herkennen van een nepwebwinkel.

Inleven in de doelgroep

Met experts is verder ingegaan op deze casus waarbij gefocust werd op twee doelgroepen; een oudere vrouw en iemand van 20 – 40 jaar oud.

Tijdens een groepsdiscussie kwam naar voren dat een oudere vrouw waarschijnlijk liever een product in een fysieke winkel koopt omdat ze onrust en onzekerheid voelt, bedachtzaam is en veel dingen online niet goed meer kan bevatten. De oudere vrouw vraagt zich ook af of het eigenlijk wel veilig is om online een aankoop te doen en vraagt liever of de (klein)kinderen het product voor haar kunnen bestellen.

Voor de 20-40'er kwam naar voren dat deze over het algemeen meer ervaren, kritischer maar ook naïever is. De 20-40'er zal vaker reviews opzoeken en een risico analyse maken (is de prijs het waard om uit te proberen of het product aankomt of niet?). Ook zal vaker bij buitenlandse webshops via creditcard of Paypal worden betaald en deze persoon maakt zich meer zorgen over 'komt een product wel aan?' dan over 'wat gebeurt er met mijn gegevens?'.

Oplossingen genereren

Vervolgens is besproken hoe we kunnen zorgen voor een digitaal inclusieve samenleving waarbij online winkelen en de angst voor nepwebwinkels niet langer een probleem hoeft te zijn. Een van de oplossingen die naar voren kwam en breed gedragen werd onder de experts was **alle bedrijven die online producten willen verkopen moeten geïdentificeerd worden**. Hiermee werd een soort e-herkenning bedoeld. Deze identificatie zou dan op persoonsniveau gedaan moeten worden en niet op bedrijfsniveau. Dus het is niet mogelijk om zomaar een webwinkel te starten, er moet altijd een

individu achter het bedrijf zitten die te allen tijde aansprakelijk is. Zo kunnen we ervoor zorgen dat een bedrijf niet als "lege entiteit" geregistreerd is. Box 4.1 toont alle genoemde oplossingen/aanbevelingen.

Box 4.1 Alle aangedragen oplossingen uit de *wishful thinking* methode

- **Alle** bedrijven die online een webwinkel beginnen worden gecheckt. Dus een soort e-herkenning. Zo komen er geen nepwebwinkels meer. Deze identificatie wordt ook gedaan op persoonsniveau, dus niet op bedrijfsniveau. Dus je kan niet zomaar een webwinkel starten, er zit altijd een individu achter die aansprakelijk is. Zo zorg je ervoor dat een bedrijf niet als lege entiteit geregistreerd is.
- Er zijn **geen** malafide verkopers meer.
- Er komt een **checklist** voor de gebruiker bij eerste bezoek website, dus bezoekers controleren of de website betrouwbaar is.
- Er zijn **zware straffen** voor de personen achter de malafide websites. Omdat alle webshops online geïdentificeerd zijn, is het oppakken van fraudeurs ook makkelijker. Er kan hierdoor in de toekomst ook voor gezorgd worden dat deze personen niet opnieuw een webwinkel mogen starten.
- Er komt een **keurmerk** op de websites en een **SOS telefoonnummer.**
- Er komt een **grote campagne** waar burgers geattendeerd worden op problemen en oplossingen. Een campagne die (ouderen) leert over online winkelen, online betalen, online veiligheid en de punten waarop gelet moet worden tijdens online aankopen doen. Hierdoor komt er meer kennis en meer bewustwording en worden mensen ook zelfverzekerder.

4.2.2 Casus 2 – phishing

Bij de tweede casus werd ingezoomd op het herkennen van phishing. Uit de vragenlijst bleek dat mensen niet zo goed onderscheid weten te maken tussen verschillende soorten berichten (wel of geen phishing). Verder blijkt dat mannen minder goed zijn in het herkennen van phishing berichten. Opvallend is verder dat leeftijd of opleidingsniveau geen rol speelt en dit dus een probleem van alle leeftijden en achtergronden lijkt te zijn.

Inleven in de doelgroep

De experts werd weer gevraagd om te focussen op twee doelgroepen; een man van middelbare leeftijd en iemand die geen hulp durft te vragen.

Tijdens een groepsdiscussie kwam naar voren dat mannen van middelbare leeftijd erg in reactie verschillen. De een vraagt zich af of de mail wel klopt, vraagt zich af wie kan helpen, checkt op spelfouten en gooit de mail weg. Andere mannen zullen zich ook afvragen of de mail wel klopt, voelen onrust, maar ook urgentie en klikken dan dus wel op het linkje. Daarna zijn ze boos of schamen ze zich als ze toch op een spam mail klikken.

Iemand die niet om hulp durft te vragen is onzeker en overrompelt, voelt stress en urgentie en weet niet wat er gedaan moet worden. Diegene zegt niks tegen de omgeving en denkt 'dit is voor mij toch veel te moeilijk'. Soms wordt de mail gelijk verwijderd, maar soms wordt ook op de link geklikt. Daarna voelen ze of trots of schaamte, afhankelijk van het resultaat.

Oplossingen genereren

Vervolgens werd gekozen om verder in te zoomen op de urgentie die gevoeld wordt bij het lezen van een phishingmail. Phishing mails komen altijd onverwacht. Hoe kunnen we er nu voor zorgen dat iemand hier niet op klikt? Een van de oplossingen die naar voren kwam en breed gedragen werd onder de experts was **een portal wat rondom het individu is ingericht.** Dat wil zeggen dat het individu zelf een portal heeft waarbij andere instanties zich moeten aansluiten. In zo'n geval zou bijvoorbeeld de Albert Heijn aan de burger moeten vragen of hij/zij de mails van de Albert Heijn wil ontvangen, in plaats van dat de mails ongevraagd verstuurd worden. Iedereen die een mail wil versturen moet **toestemming** vragen via het portal, dus een soort "mijnoverheid" met verschillende soorten gemeentes en bedrijven. Er wordt daarbij dus veel meer gedacht vanuit toestemming van de burger. Box 4.2 toont alle genoemde oplossingen/aanbevelingen.

Box 4.2 Alle aangedragen oplossingen uit de *wishful thinking* methode

- In de ideale wereld is **iedereen betrouwbaar** of is **iedereen scherp en alert.**
- Er is een systeem dat mail die je niet wil ontvangen of waarvoor je geen toestemming hebt gegeven niet toelaat in je mailbox. Je hebt dus een soort **consent** nodig. Voorbeeld: gemeenten die via mijnoverheid brieven kunnen sturen. Daar moet je eerst toestemming voor geven.
- Alle phishers kunnen worden **opgepakt** want we weten precies wie iedereen is en waar ze zich bevinden.
- Er is **wereldvrede,** geen ruimte voor ongelijkheid want er is een **basisinkomen** (en dus hoeven phishers niet te phishen).
- Er is een **special taskforce** voor phishers.
- We gebruiken **ethisch hacken** om mensen bewust te laten worden van de gevaren van spammail. Dus **ervaringsgericht leren**. Dit zorgt voor veel scherpte. Bijvoorbeeld: de overheid taskforce phishing stuurt naar iedereen een spam mail en als erop geklikt wordt krijg je te zien wat de gevolgen hadden kunnen zijn als het echt een spammail met kwade bedoelingen was geweest.
- Er is meer **hulp vanuit tech bedrijven** om dit probleem tegen te gaan. Bijvoorbeeld een programma dat de inhoud en linkjes van een email tegenleest voordat je 'm binnenkrijgt. Je legt daarbij de verantwoordelijkheid niet bij de mens (consument) maar bij de afzender en de techniek.
- **Campagne voeren** om bewustwording te creëren**,** daardoor zijn mensen sneller alert bij het lezen van hun mail.

In de focusgroep stonden het inleven in de verschillende doelgroepen en het genereren van diverse oplossingsrichtingen voor de twee belangrijkste problemen centraal. Uit de focusgroep kwamen kansrijke ideeën voor oplossingsrichtingen naar voren die nog verder uitgewerkt dienen te worden en waar vervolgonderzoek voor nodig is.

5 Conclusie

Het doel van dit onderzoek was om voor de verschillende soorten kritische vaardigheden (informatie, communicatie, content creatie) in kaart te brengen en inzichtelijk te maken tegen welke problematiek verschillende doelgroepen aan lopen en of er splintervaardigheden zijn onder verschillende doelgroepen. Om dit te achterhalen is in dit onderzoek een innovatieve multi-methodische aanpak gekozen waarin zowel diepte interviews als focusgroepen met experts (inclusief design thinking) én een grootschalig vragenlijstonderzoek onder een representatieve steekproef zijn uitgevoerd. We onderzochten zowel de eigen inschatting van digitale vaardigheden van mensen als de daadwerkelijke (kritische) digitale vaardigheden, door mensen verschillende taken uit te laten voeren. Dit geeft een uitgebreid en uniek beeld van zowel de gepercipieerde als ook de daadwerkelijke (kritische) digitale vaardigheden evenals de problemen waar verschillende doelgroepen tegenaan lopen.

5.1 Welke (kritische) digitale vaardigheden missen verschillende subdoelgroepen? En, waarom?

In dit onderzoek lag de focus op mensen met enige digitale vaardigheden (in meer of mindere mate). Voor mensen met **weinig digitale vaardigheden** zagen we dat zij op veel vlakken kennis van en ervaring met online zaken missen; zoals het kopen van producten, administratie of bankzaken. Zo kwam uit de interviews duidelijk naar voren dat deze groep de dingen graag zoveel mogelijk offline regelt. Deze groep ziet de noodzaak van het aanleren van digitale vaardigheden wel in, maar ervaart allerlei drempels. De belangrijkste reden om de dingen niet online te regelen is de angst om het verkeerd te doen. Toch is het belangrijk voor een digitaal inclusieve samenleving om deze barrières te doorbreken.

Angst en schaamte

Voor de groep mensen mét digitale vaardigheden bleek dat de **knoppenkennis** uitgebreid aanwezig was, ook waren ze veelal **overtuigd van de eigen (kritische) digitale vaardigheden**. Mannen, jongeren, hoger opgeleiden, mensen zonder migratieachtergrond en niet-religieuze mensen schatten hun eigen digitale vaardigheden hoger in dan vrouwen, ouderen, lager opgeleiden, mensen met migratieachtergrond en mensen met religie.

Bijna een derde van de respondenten ervaart **angst** bij online zaken, bijvoorbeeld dat iemand geld kan stelen als ze online persoonlijke gegevens afstaan of over dat zijn/haar apparaat wordt gehackt. Zo'n 1 op de 5 respondenten is vaak bezorgd dat ze online iets verkeerds doen en dat nadelige gevolgen heeft, dat zijn/haar online identiteit misbruikt wordt, dat ze slachtoffer worden van fraude met online bankieren of dat de dingen die ze online bestellen niet bezorgd worden. Daarnaast blijkt dat iets minder dan 1 op de 10 respondenten **schaamte** ervaart omdat zij niet weten hoe ze iets op een bepaald apparaat moeten doen. Minder dan 5% van de respondenten **durft geen hulp te vragen** en/of wil niet dat anderen te weten komen dat ze iets online niet kunnen. Over het algemeen blijkt dat vrouwen, 55+'ers, lager opgeleiden, mensen met een migratieachtergrond, mensen die thuis geen Nederlands spreken en mensen die niet werken of studeren meer angst ervaren; en dat lager opgeleiden, mensen met een migratieachtergrond, mensen die niet werken of studeren en mensen

zonder partner meer schaamte ervaren wanneer het gaat om hun digitale vaardigheden. Mensen in de leeftijd van 25-34 jaar ervaren het minste schaamte om hun eigen digitale vaardigheden.

Kritische informatievaardigheden

Uit dit onderzoek kwamen twee belangrijke problemen naar voren voor de digitale samenleving: mensen zijn niet goed in het herkennen van een nepwebwinkel en het herkennen van phishing berichten. Het niet kunnen herkennen van een nepwebwinkel speelt onder een relatief grote groep van de bevolking (ouderen en vrouwen) en het herkennen van phishing berichten lijkt over alle groepen heen te spelen. Op deze problemen gaan we daarom het meest uitgebreid in.

Een van de kernproblemen dat uit dit onderzoek naar voren kwam is dat mensen *denken* dat ze een **nepwebwinkel** goed kunnen herkennen, maar ze in de praktijk *niet goed nazoeken* of een website echt onbetrouwbaar is en dat ze vervolgens *de nepwebwinkel niet kunnen herkennen*. Met name vrouwen en ouderen (65+) hebben hier meer moeite mee. Onder bijna een derde van de respondenten leeft er een angst om slachtoffer te worden van een aankoop bij een nepwebwinkel. Een probleem dat hier bij aansluit en in de interviews naar voren kwam is dat het regelmatig voorkomt dat een besteld product niet geleverd wordt of van tegenvallende kwaliteit is. Digitaal vaardigen calculeren dit soort risico's in bij het doen van online aankopen. Voor een digitaal inclusieve samenleving is het echter belangrijk dat *iedereen* de mogelijkheid heeft om online te winkelen en dat de angst voor nepwebwinkels niet langer een probleem is. Een van de oplossingen die naar voren kwam in een expertsessie was het uitbannen van nepwebshops door alle bedrijven die online producten willen verkopen zich te laten identificeren (een soort e-herkenning met identificatie op persoonsniveau in plaats van bedrijfsniveau). Andere oplossingen zijn een checklist voor gebruikers zodat men kan controleren of een website betrouwbaar is, meer bewustzijn creëren voor het checken van keurmerken op websites; en campagnes die (ouderen) leren over online winkelen, betalen en online veiligheid. Zo'n cursus zou er met name op gericht moeten zijn om inzicht te geven in waarop iemand moet letten tijdens het doen van online aankopen.

Een ander kernprobleem dat naar voren kwam uit dit onderzoek is het **herkennen van phishing berichten**. Mensen weten niet goed onderscheid te maken tussen verschillende soorten berichten (wel of geen phishing). Mannen zijn minder goed in het herkennen van phishing berichten. Opvallend is dat leeftijd of opleidingsniveau geen rol speelt en dit dus een probleem van alle leeftijden en achtergronden lijkt te zijn. Wel blijkt dat mensen die goed waren in het herkennen van phishing berichten meer knoppenkennis hebben en (iets) meer kritische informatievaardigheden en dat zij minder schaamte ervaren (omtrent dingen die zij digitaal niet goed kunnen). Ook uit de interviews blijkt dat men het lastig vindt om phishing e-mails te herkennen als deze zeer realistisch zijn en rondom tijdstippen verstuurd worden waarop e-mails van bepaalde instanties verwacht worden (bijv. rondom de Belastingaangifte). Ondanks dat het goed is dat mensen scherp en kritisch zijn op phishing berichten, identificeren zij niet alles als phishing en in sommige gevallen zelfs onterecht. Hierdoor blijft het lastig om te bepalen wat goed/fout en betrouwbaar is. Een van de oplossingen die in de expertsessie naar voren kwam was een berichtenportal dat rondom het individu is ingericht. Er wordt daarbij dus veel meer gedacht vanuit toestemming van de burger. Andere oplossingen die genoemd werden zijn programma's die de inhoud en linkjes in een email tegenlezen en een campagne om bewustwording te creëren waardoor men sneller alert is bij het lezen van een email. Een andere manier

om meer bewustwording te creëren is ethisch hacken. Men leert ervaringsgericht wat de gevolgen zijn als ze op een linkje klikken in een (fictief) phishingbericht. Men krijgt dan meteen meer achtergrondinformatie over phishingberichten.

Als we kijken naar **andere kritische informatievaardigheden**, zoals het uitvoeren van een zoekopdracht of het herkennen van nepnieuws, blijkt dat dit taken zijn die minder problematisch zijn, maar wel problemen opleveren voor bepaalde subgroepen. Het uitvoeren van een zoekopdracht is voor een op de 10 respondenten lastig, dat komt omdat zij het lastig vinden een zoekmachine te openen en/of de juiste zoektermen te bepalen. Met name vrouwen en lager opgeleiden hebben meer moeite met het uitvoeren van een zoekopdracht, net als mensen met een migratieachtergrond. Men kan over het algemeen wel onderscheid maken tussen nepnieuws en legitieme nieuwsberichten. Toch kan ook bewustwording op dit vlak vergroot worden. Ongeveer een vijfde van de mensen gaat er namelijk vanuit dat al het online nieuws betrouwbaar is en 1 op de 4 mensen trekt een nieuwsbericht *niet* na bij twijfel. Uit de interviews kwam ook naar voren dat men snel aanneemt dat al het nieuws betrouwbaar is. Ook nu zijn lager opgeleiden minder goed in het herkennen van nepnieuws. Ouderen (65+) zijn hier juist beter in.

Het onder de aandacht brengen van nepnieuws en het kritisch blijven evalueren van informatie blijft belangrijk. Mensen herkennen nepnieuws wel maar een groot deel checkt bij twijfel niet of een bericht wel echt betrouwbaar is. Met het oog op recente ontwikkelingen zoals het programma ChatGPT blijft dit een belangrijk aandachtspunt. ChatGPT is een chatbot met kunstmatige intelligentie en gespecialiseerd in het voeren van dialogen met een gebruiker. ChatGPT wordt echter ook misbruikt om nepnieuws te genereren.[72]

Dit onderzoek biedt inzicht in welke verklarende factoren er zijn voor het (niet) kunnen herkennen van phishing berichten en nepwebwinkels – de indicatoren voor oorzaken van (ontbrekende) digitale vaardigheden, privacy attitude en de persoonskenmerken. Het geeft dus inzicht in de barrières die een rol spelen bij het (niet) kunnen uitvoeren van digitale taken. Er is echter vervolgonderzoek nodig om interventies en campagnes, gericht op het herkennen van phishing berichten en nepwebwinkels, goed aan te laten sluiten bij de skills set en het doenvermogen van verschillende groepen burgers. Informatie moet opvallen en men moet de informatie goed begrijpen en vertrouwen. Door de effectiviteit van interventies of campagnes te toetsen onder (een representatieve groep) burgers wordt inzicht verkregen in welke elementen goed werken en welke eventueel nog doorontwikkeld moeten worden.

Kritische communicatievaardigheden en content creatievaardigheden

Als we kijken naar de **kritische communicatievaardigheden** dan laat dit onderzoek zien dat mensen over het algemeen goed weten welke berichten zij niet zomaar online mogen delen zonder hier toestemming voor te vragen aan anderen. Ouderen (65+) zijn hier iets minder goed in, net zoals lager opgeleiden. Uit de interviews kwam duidelijk naar voren dat het onder de jongere generatie veel gebruikelijker is om elkaar om toestemming te vragen voordat foto's geplaatst worden en ook denken jongeren uitgebreider na over de consequenties van de content die zij plaatsen.

[72] Link naar nieuwsartikel

Tot slot, als we kijken naar de **kritische content creatievaardigheden** valt op dat jongeren sneller akkoord zijn en het ook nuttig vinden dat zoekresultaten gepersonaliseerd worden. Waar jongeren het nuttig en oké vinden om gepersonaliseerde zoekresultaten op basis van locatie te krijgen of op basis van eerdere zoekopdrachten zijn mensen ouder dan 55 jaar hier terughoudender in. Bovendien blijkt dat hoe bezorgder men is over de eigen privacy, hoe minder acceptabel men het gebruik van gegevens voor personalisering vindt. Uit de interviews kwam naar voren dat men het soms best handig vindt dat informatie gepersonaliseerd is en dat men ook maar accepteert dat dit zo is ("ik heb toch niets te verbergen"), maar het ook een beetje beangstigend vindt. Men weet ook niet goed hoe hiermee om te gaan.

Splintervaardigheden

Het niet kunnen herkennen van nepwebwinkels en phishing berichten zijn problemen die in grote groepen lijken te spelen. Ook binnen subgroepen zijn er echter verschillen in digitale vaardigheden. Sommige mensen hebben bepaalde digitale vaardigheden wel sterk ontwikkeld en andere digitale vaardigheden niet, dit worden *'splintervaardigheden'* genoemd. Figuur 5.1 geeft een overzicht van de splintervaardigheden van verschillende subdoelgroepen.

Figuur 5.1 Verschillen in kritische digitale vaardigheden tussen verschillende subdoelgroepen

	Zoekopdracht uitvoeren	Nep-webwinkel herkennen	Nepnieuws herkennen	Phishing bericht herkennen	Adequaat social mediagebruik	Filterbubbel
Geslacht						
Man	+	+		-		
Vrouw	-	-		+		
Leeftijd						
Jongeren		+	-		+	-
Ouderen (soms 55 en ouder, soms 65 en ouder)		-	+		-	+
Opleiding						
Laag	-		-		-	-
Hoog	+		+		+	+
Stedelijkheid						
Niet stedelijk	+					
Stedelijk	-					
Regio						
Noord				-		
Zuid				-		
Oost				+		
West				+		
Migratieachtergrond (1e en 2e; Westers en Niet-Westers)						
Nee	+					
Ja	-					
Religieus						
Nee						
Ja						
Thuis geen Nederlands spreken						
Nee						
Ja						
ZZP'er						
Nee						
Ja						
Geen werk of aan het studeren						
Nee						
Ja						
Geen partner						
Nee						
Ja						

Per taak is aangegeven welke subdoelgroepen minder goed of juist beter zijn in het uitvoeren dan de taak. Rode vakken (met een minteken) geven aan dat een bepaalde groep minder goed is in het uitvoeren van een bepaalde taak. Groene vakken (met een plusteken) geven aan dat een bepaalde groep hier beter in is. Als de vakken geen kleur hebben dan betekent dat dat een bepaalde groep het niet beter of minder goed doet dan andere groepen. Zo speelt religie, het spreken van een andere taal thuis, het niet hebben van werk of studie, ZZP'er zijn, of het niet hebben van een partner wel of geen rol in het goed uit kunnen voeren van de taken.

Uit dit onderzoek komen de volgende splintervaardigheden naar voren bij verschillende subdoelgroepen:

- Vrouwen weten goed een phishing bericht te herkennen maar zijn minder goed in het uitvoeren van een zoekopdracht en het herkennen van een nepwebwinkel, voor mannen is dit precies andersom. Een verklaring hiervoor kan zijn dat mannen wellicht sneller de urgentie voelen om op een link in een phishing bericht te klikken en vrouwen wellicht kritischer lezen. Ander onderzoek laat echter gemixte resultaten zien wat betreft de rol van geslacht bij het herkennen van phishing berichten. Uit sommige onderzoeken blijkt dat gender helemaal geen rol speelt, uit andere onderzoeken blijkt weer dat mannen beter zijn in het herkennen van phishing berichten dan vrouwen.
- Jongeren ervaren geen angst en schaamte en weten goed wat ze online wel en niet kunnen delen op social media. Zij vinden het ook minder erg dat zoekresultaten gepersonaliseerd worden. Jongeren zijn echter niet zo goed in het herkennen van nepnieuws.
- Lager opgeleiden hebben meer moeite met bijna alle taken, zij weten niet zo goed hoe ze een zoekopdracht uit moeten voeren, hoe ze nepnieuws moeten herkennen en hoe ze social media moeten gebruiken. Zij vinden het ook minder erg dat resultaten gepersonaliseerd worden. Dat lager opgeleiden minder digitaal vaardig zijn blijkt ook al uit veel eerdere onderzoeken.[73]
- Mensen die in een stad wonen zijn minder goed in het uitvoeren van een zoekopdracht. En mensen die in de regio Noord- of Zuid-Nederland wonen zijn minder goed in het herkennen van phishing berichten.
- Tot slot blijkt dat mensen met een migratieachtergrond minder goed zijn in het uitvoeren van een zoekopdracht. Een verklaring hiervoor kan zijn dat hier een goede beheersing van de Nederlandse taal voor nodig is en de onlinetaalvaardigheden bij deze groep waarschijnlijk achter blijven.[74] Opvallend is ook dat mensen met een migratieachtergrond niet meer problemen op de andere taken ervaren dan mensen met een autochtone achtergrond.

5.2 Welke leerbehoefte is er en hoe wil men graag leren?

Men vindt het belangrijk om meer te leren over het beschermen van de online privacy en hoe men online fraude kan herkennen. Dit sluit goed aan bij de problematiek die naar voren komt rondom het herkennen van nepwebwinkels en phishing berichten en die in dit onderzoek nader verkent is in fase 3. Ook het aanleren van de meer praktische vaardigheden wordt vaker genoemd, zoals het bewerken van

[73] Zie bijvoorbeeld: Van Deursen, A.J.A.M. (2018). Digitale ongelijkheid in Nederland anno 2018. Enschede, Nederland: Universiteit Twente. En: Ingen, E. & Haan, Jos & Duimel, M. (2008). Achterstand en afstand. Digitale vaardigheden van lager opgeleiden, ouderen, allochtonen en inactieven. Revista Panamericana De Salud Publica-pan American Journal of Public Health - REV PANAM SALUD PUBLICA.

[74] Link naar didactiek Nederlands

foto's en/of video's, het gebruik van een bepaalde programmeertaal en het maken van een website. Over het algemeen gaven jongeren vaker aan een programmeertaal te willen leren en was voor 35 en ouder het herkennen van online fraude belangrijker. Men leert het liefst via een handleiding op internet, via filmpjes van Youtube of een op een van een vriend of familielid.

5.2 Aanbevelingen

Mensen met weinig digitale vaardigheden ervaren allerlei barrières als het gaat om digitale zaken en vaardigheden. Er is een sterke angst om dingen verkeerd te doen. Door de toenemende digitalisering is het van belang dat ook deze groep niet digitaal vaardigen volwaardig mee kan blijven doen aan de samenleving. Voor deze groep is het belangrijk om niet-digitale alternatieven aan te blijven bieden, bijvoorbeeld een telefoonnummer voor hulp bij problemen in plaats van een app of een chatbot. Ook is educatie van basis digitale vaardigheden belangrijk voor deze groep. Dit is een vereiste om complexere digitale taken uit te kunnen voeren, zoals het doen van een online aankoop of het kunnen werken met een DigiD. Bij het uitvoeren van complexere digitale taken hebben zij veel hulp, uitleg en herhaling nodig. Cursusaanbod dat aansluit bij deze aspecten is al volop beschikbaar en dit aanbod blijft dan ook belangrijk.

Dit onderzoek laat zien dat er onder verschillende subdoelgroepen splintervaardigheden voorkomen. Men is dan digitaal vaardiger in één context maar loopt tegen problemen aan in een andere context. Dit onderzoek geeft handvaten om gerichter educatieprogramma's en bewustwordingsstrategieën onder verschillende doelgroepen in te zetten. Zo is het belangrijk om extra aandacht aan lager opgeleiden te geven wanneer het gaat om alle digitale vaardigheden. Daarnaast is het belangrijk om mensen met een migratieachtergrond (en mogelijk ook een taalachterstand) te ondersteunen met de kritische informatievaardigheden en dan met name het uitvoeren van zoekopdrachten.

Toch komt in dit onderzoek vooral duidelijk naar voren dat het nog veel belangrijker is om te focussen op de twee grootste problemen voor mensen: het herkennen van phishing berichten en nepwebwinkels. Een aanzienlijk deel van de mensen heeft hier moeite mee maar ziet zelf niet in dat ze hier moeite mee hebben. Bovendien spelen deze uitdagingen onder een groot deel van de Nederlandse bevolking en lijken dan ook een probleem van alle leeftijden en achtergronden te zijn. Veel mensen denken dus dat ze dit goed kunnen, maar kunnen dit in de praktijk niet. In een wereld waarin het aantal nepwebwinkels en phishing berichten toeneemt is het dan ook noodzakelijk om bewustzijn van deze problematiek te vergroten en mensen digitaal vaardiger te maken op deze vlakken. Wij raden dan ook aan om sterk in te zetten op interventies gericht op het vergroten van bewustwording rondom het herkennen van phishingberichten en nepwebwinkels, of het systeem hier anders op in te richten.

Samenvattend, biedt dit onderzoek inzicht in factoren die een rol spelen bij het (niet) kunnen uitvoeren van digitale taken en biedt handvaten voor doelmatig, doeltreffend en proportioneel beleid voor een digitale samenleving waarin zoveel mogelijk burgers voldoende vaardigheden kunnen ontwikkelen om mee te kunnen (blijven) doen.