DIGITALE VEILIGHEID BINNEN HET PO

Een onderzoek vanuit het lectoraat Cybersecurity & Safety van De Haagse Hogeschool

let's change
YOU. US. THE WORLD.

INFORMATIEPAKKET BASISSCHOLEN

M. Maris & E. van den Brink

-Versie 26-01-2021-

DE HAAGSE HOGESCHOOL

Voorwoord

Voor u ligt het informatiepakket voor basisscholen waarin wordt toegelicht op welke wijze we de benodigde onderzoeksgegevens onder de kinderen en leraren van de groepen 7 en 8 op uw school graag willen verzamelen.

De informatie zal in principe door een student uit het aan uw school verbonden kernteam van de Pabo in de vorm van een intake worden geïntroduceerd waarbij de processen van de afname van de vragenlijsten, het houden van de interviews en het gebruik van de app worden toegelicht en sluitende afspraken kunnen worden gemaakt over de uiteindelijk te volgen procedure (wie doet wat op welk moment en op welke manier?) van de afname, de afnamedata en andere zaken die binnen het onderzoek van belang zijn.

Vervolgens zal de student zoveel mogelijk zorgdragen het verzamelen van de data middels een vragenlijst voor de leerlingen van de groepen 7 en 8 en een interview voor hun leraren. Ook kan indien de situatie daarom als alternatief een app worden ingezet.

We willen u alvast enorm bedanken voor uw medewerking.

Schroom in geval van vragen, opmerkingen, niet om contact met ons opte nemen.

Met vriendelijke groeten,

Marinus Maris en Erik van den Brink.

M. Maris
E-mailadres: m.g.maris@hhs.nl.

E. van den Brink
E-mailadres: e.vandenbrink@hhs.nl.

Inhoudsopgave

Achtergrondinformatie

'…Het afgelopen jaar steeg het aantal politie-aangiftes van cybercrime met 66%, kregen ondernemers en kennisinstellingen te maken met gijzelsoftware en liep de economische schade hierdoor navenant op. Desondanks vinden Nederlanders zelf dat zij goed op de hoogte zijn van hun digitale veiligheid en schatten de kans dat zij schade ondervinden door onveilig online gedrag laag (10%) in. Bovendien is de behoefte bij Nederlanders die aantoonbaar achterlopen op online veilig gedrag om zichzelf te verbeteren, eveneens laag. Dat blijkt uit Veilig Online 2020, het jaarlijkse onderzoek naar het bewustzijn van Nederlanders rondom cybersecurity…' (van der Grient et al., 2020)

Het is dan ook evident, dat de overheid de noodzaak en het belang van de bewustwording hiervan en kennis daarover verder wil stimuleren. Dit gebeurt onder meer in de vorm van Alert Online, een jaarlijkse campagne van overheid, bedrijfsleven en wetenschap met als doel Nederland bewuster en veiliger online te laten zijn. Ook is zoals ongetwijfeld bekend in opdracht van de overheid onder de noemer '*curriculum.nu*' (Curriculum.nu, 2018) een traject gestart dat uiteindelijk moet leiden tot een herziening van het curriculum voor het primair en voortgezet onderwijs. Digitale Geletterdheid is daarbij een van de in totaal negen leergebieden die de basis gaan vormen voor het onderwijsprogramma van de toekomst.

Uit het bovengenoemde onderzoek blijkt bijvoorbeeld dat er *'…een duidelijk verschil is tussen Nederlanders die écht goed op de hoogte zijn van de technische kanten van het internet en degenen die de digitale wereld omarmen als onderdeel van het sociale leven. De eerste groep deelt liever niet (te) veel informatie over zichzelf online, omdat ze goed op de hoogte zijn van wat er allemaal met persoonlijke data kan worden gedaan. De laatste groep is lang niet altijd op de hoogte van digitale risico's of wil deze niet zien. Zij vinden het geen probleem om informatie over zichzelf online te delen. Deze veelgebruikers van bijvoorbeeld sociale media vinden discussies over privacy ingewikkeld, overzien daarvan de gevolgen niet en menen er dus geen last van te hebben. Ze gaan de risico's van hun gedrag liever uit de weg en lopen dus relatief veel gevaar…'* Verder blijken ouderen over minder up-to-date kennis te beschikken terwijl ze *'…tegelijkertijd hun eigen kennis en overschatten daardoor hun persoonlijk gevaar…'* Jongeren blijken daarentegen *'…beter op de hoogte, maar onderschatten desondanks hun persoonlijke gevaren waardoor zij ook slachtoffer worden van internetcriminaliteit*…' (van der Grient et al., 2020)

Wat betreft het nieuwe curriculum hebben de leraren en schoolleiders in de loop van 2019 hun opbrengsten aangeboden aan minister Slob. Ze vormen het vertrekpunt om te komen tot concrete onderwijsdoelen. Een wetenschappelijke commissie heeft de taak gekregen het kabinet ten aanzien van genoemde opbrengsten te adviseren over het vervolgproces van de curriculumherziening. Na dit advies heeft de Stichting Leerplan Ontwikkeling (SLO, 2018) i.s.m. Curriculum.nu de voorstellen vertaald naar concrete onderwijsdoelen. De concepten die hieruit zijn voortgekomen zullen naar verwachting in de schooljaren 2021-2022 en 2022-2023 middels enkele pilots worden getoetst, waarna op basis van het uiteindelijke advies van de wetenschappelijke commissie medio 2023 de herziene doelen voor het primair onderwijs in een wetsvoorstel aan de Tweede Kamer worden voorgelegd.

Het lectoraat Cybersecurity & Safety van de Haagse Hogeschool houdt zich bezig met maatschappelijke thema's rondom cybersecurity. In dat kader is vanuit het lectoraat het onderzoek *'Digitale Veiligheid binnen het PO'* geïnitieerd dat deels wordt gesubsidieerd door het Regieorgaan Praktijkgericht Onderzoek (SIA).

Het onderzoek richt zich op het digitaal veilig gedrag van leerlingen op de basisschool en hun leraren. Na een gedegen literatuurstudie zijn een vragenlijst voor de kinderen uit de groepen 7 en 8 en een interview voor hun leraren ontwikkeld. Mede als gevolg van het Covid-19 virus, waarwe het afgelopen jaar mee zijn geconfronteerd, is daarnaast een app ontwikkeld welke als alternatief binnen het proces van dataverzameling kan worden ingezet.

Op basis van de opbrengsten worden interventies ontwikkeld die binnen de participerende scholen worden uitgezet. De effectiviteit van de interventies wordt geanalyseerd met effectmetingen.

De **centrale onderzoeksvraag** luidt:
Welke factoren zijn bepalend voor de mate van veilig digitaal gedrag onder basisscholieren van groep 7 en 8 en hoe zijn deze effectief te beïnvloeden?

De **deelvragen** daarbij zijn:

- Welke factoren zijn bepalend voor het niveau van veilig digitaal gedrag van de doelgroep.
- In welke mate zijn deze factoren beïnvloedbaar?
- Welke interventies zijn geschikt om het niveau van veilig digitaal gedrag te verhogen?
- Hoe kunnen deze interventies ontwikkeld worden?
- Hoe effectief zijn deze interventies in de praktijk?

Binnen dit onderzoek worden de volgende **activiteiten** uitgevoerd:

- **Het benaderen van de doelgroep voor dit onderzoek**
  Het onderzoek richt zich op het digitaal veilig gedrag van leerlingen op de basisschool en hun leraren. Aanvankelijk betreft het zogenoemde convenantscholen waarmee de Pabo van DeHaagse Hogeschool samenwerkt. De scholen worden met behulp van de stagecoördinator en de instituutsopleiders van de Pabo binnen de bestaande kernteams met studenten benaderd om toestemming te vragen, ook van de ouders, voor deelname aan het onderzoek.
- **Het uitvoeren van de nulmeting om het huidige niveau van veilig digitaal gedrag te meten**
  Binnen het lectoraat is hiervoor een meetmethode ontwikkeld. Deze is gebaseerd op een uitgebreide enquête welke zich met name richt op de risicoperceptie, risicoattitude en het beveiligingsgedrag met betrekking tot het gebruik van digitale media en sociale netwerken. Hiertoe zijn in totaal drie onderzoeksinstrumenten beschikbaar, te weten een vragenlijst voor de leerlingen uit de groepen 7 en 8 en een set met interviewvragen voor hun leraren ontwikkeld. Als gevolg van de perikelen rondom Covid19, waar we het afgelopen jaar mee zijn geconfronteerd, is daarnaast een app ontwikkeld welke als alternatief binnen het proces van dataverzameling kan worden ingezet. In principe is het de bedoeling dat studenten van de Pabo de data op hun opleidingsschool verzamelen.
- **Het onderzoeken naar de factoren die van invloed zijn op het niveau van veilig digitaal gedrag van kinderen en welke daarvan beïnvloedbaar zijn**
  Dit wordt onderzocht door middel van een literatuuronderzoek. Ook vinden expertinterviews (didactiek, pedagogiek, gedragsbeïnvloeding, serious gaming) en enquêtes bij docenten plaats. De daarbij te volgen methodische aanpak is die van (Janssens, 1998).
- **Een onderzoek naar geschikte interventies**
  Hierbij staat de vraag hoe een interventie het best vormgegeven kan worden om een bepaalde factor te beïnvloeden centraal. Voorbeelden van interventies zijn een game, een mobiele applicatie en een website. Een literatuuronderzoek en diverse expertinterviews vormen bij dit onderdeel de instrumenten.

- Vervolg - Binnen dit onderzoek worden de volgende **activiteiten** uitgevoerd:

- **Het ontwikkelen van interventies**
  Dit gebeurt aan de hand van de Design Science methode (Hevner et al., 2004) welke zich richt op het iteratief verbeteren van het te ontwikkelen artefact. Het komt er in het kort op neer dat er door studenten onder begeleiding eerst prototypes worden ontwikkeld die worden getest en waar nodig gemodificeerd alvorens ze daadwerkelijk in de praktijk (basisschool) worden ingezet.
- **Het toepassen van de interventies in de praktijk**
  De interventies worden in de basisschoolpraktijk uitgevoerd waarbij tijdens de interventieperiodes relevante onderzoeksdata wordt verzameld.
- **Het uitvoeren van een effectmeting**
  Na het toepassen van de verschillende interventies wordt voor iedere afzonderlijke interventie een effectmeting uitgevoerd. In principe zullen daarbij dezelfde onderzoeksinstrumenten als bij de eerder beschreven nulmeting worden ingezet.
- **De rapportage van de bevindingen**
  De uitkomsten van het onderzoek worden verwerkt in een wetenschappelijke paper. Daarnaast worden beschrijvingen van de ontwikkelde interventies en onderwijsmateriaal opgeleverd.
- **Disseminatie van de projectresultaten**
  Dit gebeurt middels presentaties en publicaties in diverse vaktijdschriften. De ontwikkelde interventies worden daarbij beschikbaar gesteld aan de participerende basisscholen en andere betrokkenen.

De vragenlijsten voor de leerlingen

GEBRUIKSINSTRUCTIE

Hieronder is kort uitgelegd hoe de vragenlijst is opgebouwd en op welke wijze de vragen moeten worden afgenomen.

Voorafgaande aan de afname

- De overdracht van de onderzoeksdocumentatie vindt plaats door middel van een intakegesprek. In het bijzonder worden dan ook de procedures van de afname van de vragenlijsten en interviews toegelicht, afnamedata met elkaar afgestemd en overige afspraken gemaakt.
- Deze vragenlijst is bedoeld voor de kinderen uit de groepen 7 en 8 van het primair onderwijs en bevat in totaal 66 vragen die evenredig zijn onderverdeeld (22 onderdelen: A tot en met V met ieder 3 vragen).
- Houd rekening met een maximale afnametijd van zo'n drie kwartier tot een uur.
- De vragenlijst wordt bij voorkeur klassikaal en digitaal (pc, laptop, tablet, smartphone) afgenomen. Daarvoor is een internetverbinding vereist.
- Op verzoek is een papieren versie beschikbaar (afspraken daarover worden tijdens het intakegesprek gemaakt).
- Ook is een afname-combinatie mogelijk (wanneer bijvoorbeeld de vragen centraal op het digibord worden geprojecteerd en de kinderen de antwoorden op papier invullen (eveneens op verzoek beschikbaar).
- De kinderen beantwoorden de vragen na een korte werkinstructie (66 vragen, digitaal of op papier, wanneer starten en stoppen, ...) door de juf of meester zoveel mogelijk zelfstandig.
- De digitale afname moet in 1 keer plaatsvinden. Bij een afname op papier kan deze worden uitgesmeerd over een langere periode met enkele afname-deelmomenten.
- De vragenlijst is anoniem. Wel wordt gevraagd naar het geslacht, de leeftijd en de groep.
- De juf of meester observeert tijdens de afname en kan op verzoek verdere verduidelijking geven.
- We vragen expliciet om feedback op het proces van de afname en vernemen graag van de juf of meester (en eventueel de kinderen) hoe het is gelopen, wat wel / niet goed verliep, wat niet duidelijk (genoeg) was, et cetera. Voel u vrij om ook mogelijke oplossingen met ons te delen. Hiertoe is een evaluatieformulier beschikbaar (overdracht tijdens het intakegesprek).

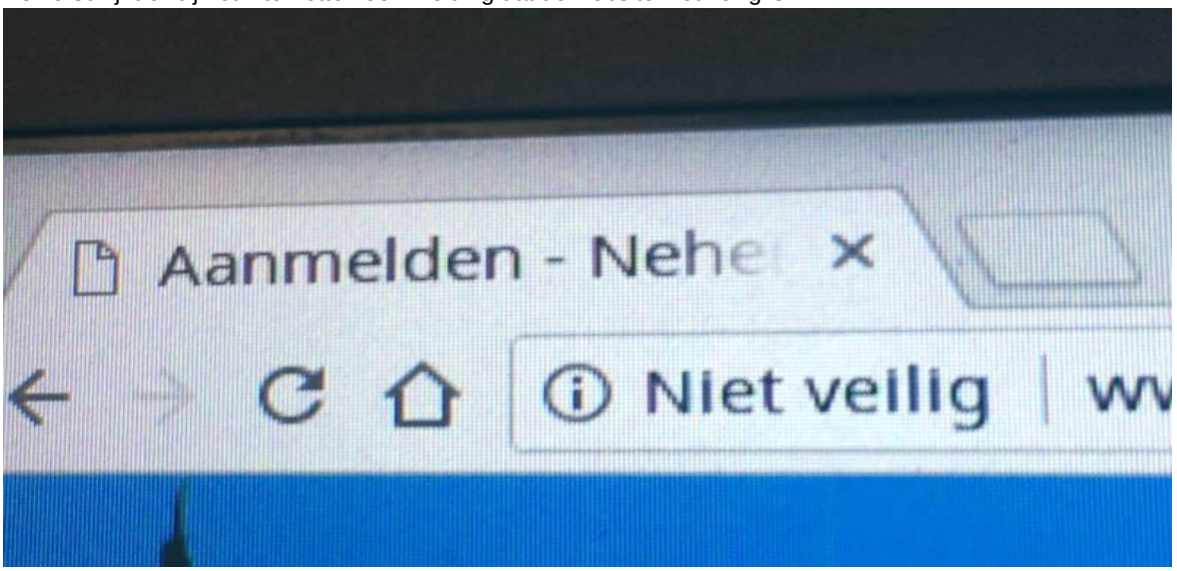
Tijdens de afname

- De kinderen beantwoorden de vragen in de aangegeven volgorde.
- Iedere pagina bevat een onderdeel dat begint met een korte tekst en een afbeelding. Dan volgen 3 vragen.
- De kinderen bekijken de afbeelding goed, lezen de tekst daarbij en beantwoorden dan de vragen.
- Zijn er vragen of onduidelijkheden mag een kind de juf of meester inschakelen.
- Graag benadrukken we het belang van de authenticiteit van de antwoorden: het kind schrijft binnen de beschikbare tijd op wat hij/zij wil, kan en weet; of een antwoord kort of lang is maakt niet uit.
- Met behulp een druk op de knop 'Volgende' navigeer je naar de volgende pagina (met het volgende onderdeel).
- Terugbladeren en het veranderen van voorgaande antwoorden is geen enkel probleem.

Na de afname

- De juf of meester laten de kinderen aan het eind van de vragenlijst voor de zekerheid controleren of alle vragen zijn ingevuld waarna de antwoorden met behulp van een druk op de knop 'Verzenden' worden verstuurd.
- Indien sprake is van een afname (deels) op papier verzamelt de juf of meester de ingevulde vragenlijsten of antwoordbladen. Als het goed is, is tijdens het intakegesprek een afspraak voor het afhalen van de data gemaakt

ONDERDEEL A	
Hoi en fijn dat je mee wilt doen aan het onderzoek over Digitale Veiligheid! We hebben eerst wat algemene gegevens van je nodig. Alvast bedankt voor het meedoen, we kijken uit naar jouw antwoorden! 	
01	**Ben je een meisje of jongen?**
02	**Hoe oud ben je?**
03	**In welke groep zit je?**

ONDERDEEL B	
Soms verschijnt er bij het internetten een melding dat de website niet veilig is.  	
04	**Wat betekent het wanneer je zo'n melding krijgt?**
05	**Wat kan er gebeuren wanneer je een niet-beveiligde website bezoekt?**
06	**Waar houd je rekening mee als je een melding krijgt van een niet-beveiligde website?**

ONDERDEEL C

Veel mensen versturen berichtjes via de chat.

07	**Als je met iemand aan het chatten bent, weet je dan altijd zeker met wie je chat?**
08	**Wat kan er gebeuren als je met iemand chat die je niet kent?**
09	**Op welke manier denk je na over veiligheid als je met iemand aan het chatten bent?**

ONDERDEEL D	
Op een website wordt de vraag gesteld om cookies te accepteren.  	
10	**Als je een website voor de eerste keer opent krijg je soms een melding om cookies te accepteren. Is dit gevaarlijk?**
11	**Wat kan er gebeuren als je cookies accepteert?**
12	**Accepteer jij cookies van de websites die je bezoekt?**

ONDERDEEL E

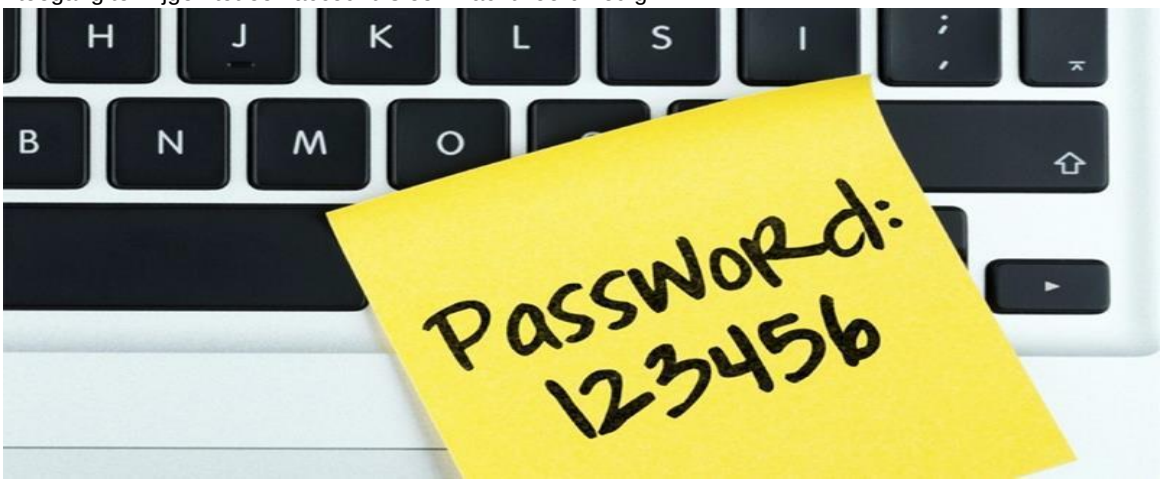
In een advertentie wordt opgeroepen om een app te downloaden en deze op je telefoon installeren.

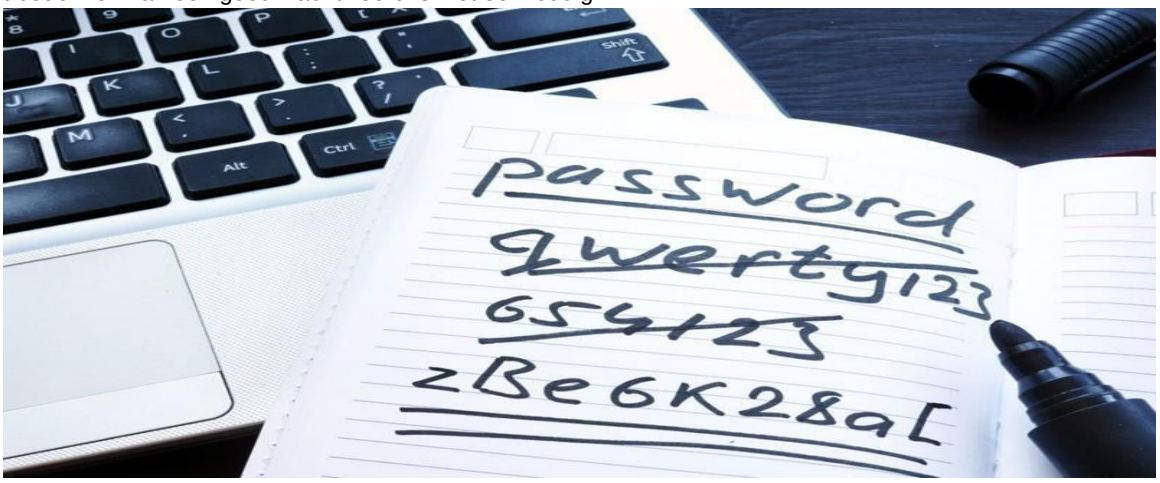
13	**Kan jouw telefoon met een virus worden besmet als je een app installeert?**
14	**Wat kan er gebeuren wanneer een telefoon is besmet met een virus?**
15	**Wat doe je wanneer je een virusmelding op je telefoon krijgt?**

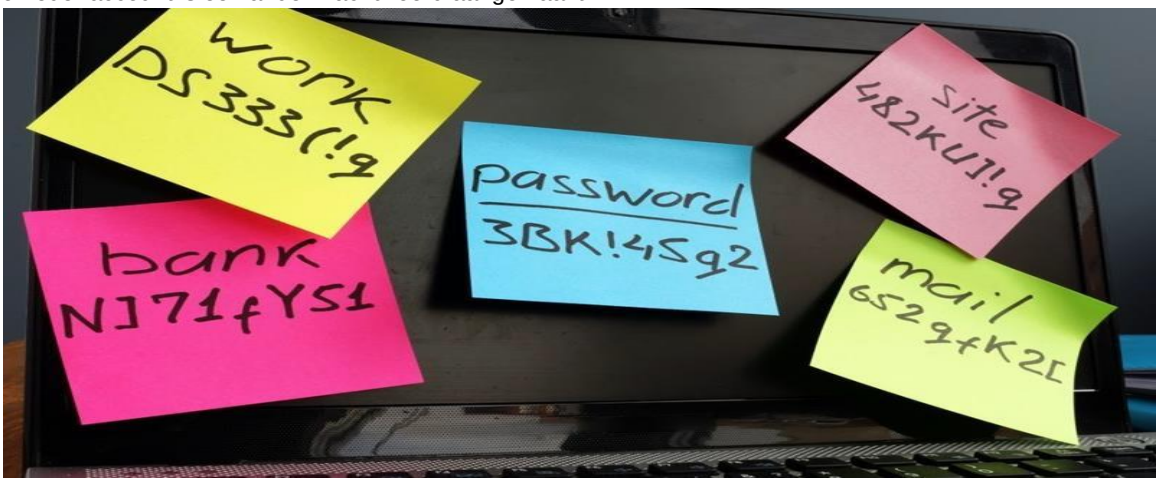
ONDERDEEL F

Een virusscanner geeft een waarschuwing bij gevaar.

16	**Moet je een virusscanner op jouw telefoon installeren?**
17	**Wat kan er gebeuren als je geen virusscanner op je telefoon hebt geïnstalleerd?**
18	**Heb je een virusscanner op je telefoon geïnstalleerd? Waarom wel/niet?**

ONDERDEEL G	
Om toegang te krijgen tot een account is een wachtwoord nodig.  	
19	**Moet je een sterk wachtwoord aanmaken voor een account?**
20	**Wat kan er gebeuren als iemand jouw wachtwoord weet?**
21	**Waar houd je rekening mee wanneer je ergens een wachtwoord moet aanmaken?**

ONDERDEEL H	
Het bedenken van een goed wachtwoord is niet eenvoudig.  	
22	**Een vriend is op zoek naar een nieuw wachtwoord. Hoe kan jij hem daarmee helpen?**
23	**Wat kan er gebeuren als je geen sterk wachtwoord gebruikt om in te loggen?**
24	**Vind je het leuk om anderen te helpen met het veiliger te maken van hun telefoon?**

ONDERDEEL I	
Voor ieder account is een ander wachtwoord aangemaakt.  	
25	**Heb je een wachtwoord-manager nodig?**
26	**Wat kan er gebeuren als je geen wachtwoord-manager gebruikt?**
27	**Gebruik jij een wachtwoord-manager? Waarom wel/niet?**

ONDERDEEL J

In een advertentie kun je een gratis tablet winnen!

28	**Waarom zou iemand zomaar een gratis tablet aanbieden?**
29	**Stel dat jij zo'n aanbieding op internet tegenkomt en je klikt erop. Krijg je de tablet dan gratis?**
30	**Wat is jouw reactie als je een advertentie op het internet tegenkomt waarin een gratis product wordt aangeboden?**

ONDERDEEL K

In berichten staat wel eens een linkje waar je op kunt klikken.

31	**Waarom zou iemand zo'n link in een bericht meesturen?**
32	**Waar houd jij rekening mee als je een bericht met daarin een link ontvangt?**
33	**In welke groep zit je?**

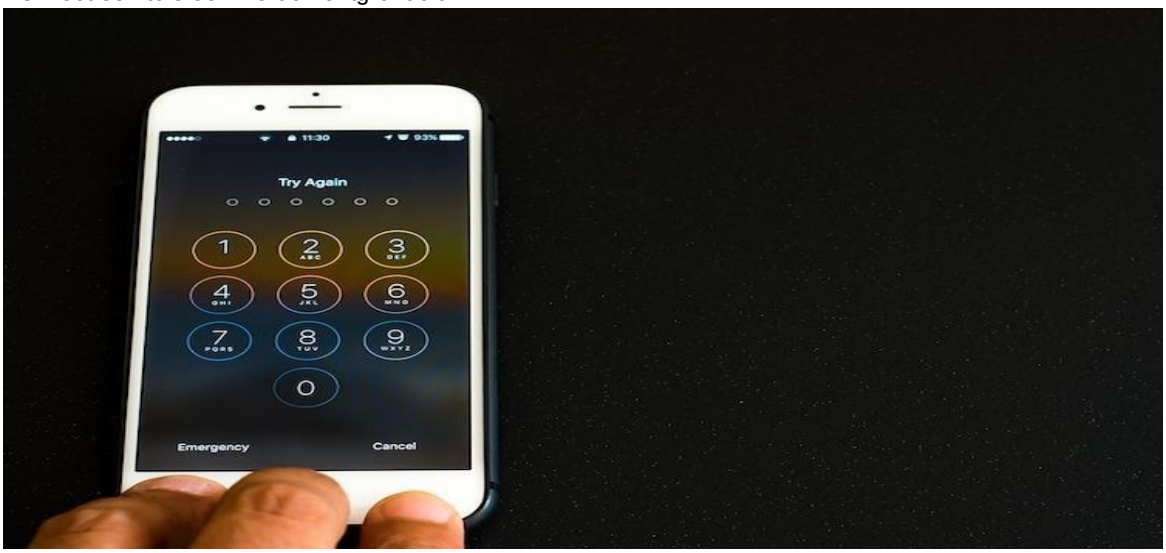
ONDERDEEL L

In een bericht vraagt iemand om geld.

34	**Als je een bericht krijgt dat je niet vertrouwt, vertel je dit dan aan jouw ouders, juf of meester?**
35	**Wat kan er gebeuren als je een bericht ontvangt dat je niet vertrouwt en dit verder aan niemand vertelt?**
36	**Wat doe je als je een bericht ontvangt dat je niet vertrouwt?**

ONDERDEEL M

Soms moet een telefoon worden ontgrendeld.

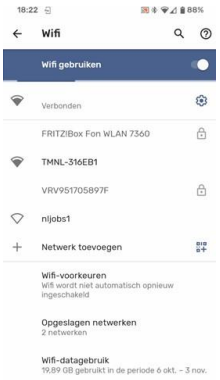


37	**Is het belangrijk om je telefoon te vergrendelen?**
38	**Wat kan er gebeuren als je je telefoon niet hebt vergrendeld?**
39	**Vergrendel jij jouw telefoon? Waarom wel/niet?**

ONDERDEEL N	
Van een app is een update beschikbaar.  	
40	**Moet je apps updaten??**
41	**Wat kan er gebeuren als je apps niet regelmatig update?**
42	**Vind jij dat de apps op jouw telefoon regelmatig moeten worden geupdate? Waarom wel/niet?**

ONDERDEEL O

Er zijn beveiligde en niet-beveiligde WiFi-netwerken.



43	**Wat kan er gebeuren wanneer je een niet-beveiligde Wifi-verbinding gebruikt?**
44	**Als je ergens een Wifi-verbinding wilt gebruiken, denk je er dan over na of dit wel veilig is?**
45	**Is het gebruiken van een niet-beveiligde Wifi-verbinding gevaarlijk?** **Waarom wel/niet?**

ONDERDEEL P

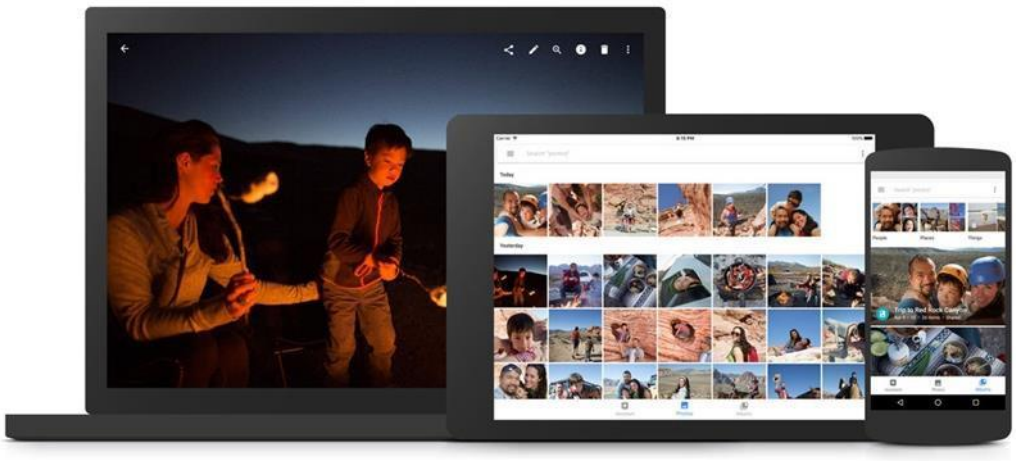
Aan een icoon is te zien dat sommige gegevens van de app zijn beveiligd.

46	**Vind je het belangrijk om de toegang tot de apps op jouw telefoon te beveiligen?**
47	**Wat kan er gebeuren als iemand ongevraagd toegang tot jouw telefoon krijgt?**
48	**Waar houd jij rekening mee als je foto's met je telefoon maakt en die wilt delen met iemand anders?**

ONDERDEEL Q

Bij het installeren van een app wordt soms gevraagd om toegang tot bepaalde onderdelen van de telefoon.

49	**Is het veilig om een app toegang te geven tot de contacten of locatie van jouw telefoon?**
50	**Wat kan er gebeuren als je een app toegang geeft tot jouw contacten of locatie?**
51	**Geef jij een app die daarom vraagt toegang tot jouw contacten of locatie?** **Waarom wel/niet?**

ONDERDEEL R	
Foto's en filmpjes kunnen in de cloud worden opgeslagen zodat je er altijd met ieder apparaat gemakkelijk bij kunt. 	
52	**Kunnen mensen de foto's of filmpjes die in de cloud zijn opgeslagen van elkaar zien?**
53	**Wat kan er gebeuren als je foto's of filmpjes in de cloud hebt opgeslagen?**
54	**Heb jij zelf wel eens foto's of filmpjes in de cloud opgeslagen? Waarom wel/niet?**

ONDERDEEL S

Profielgegevens in jouw apps kunnen door anderen worden bekeken.

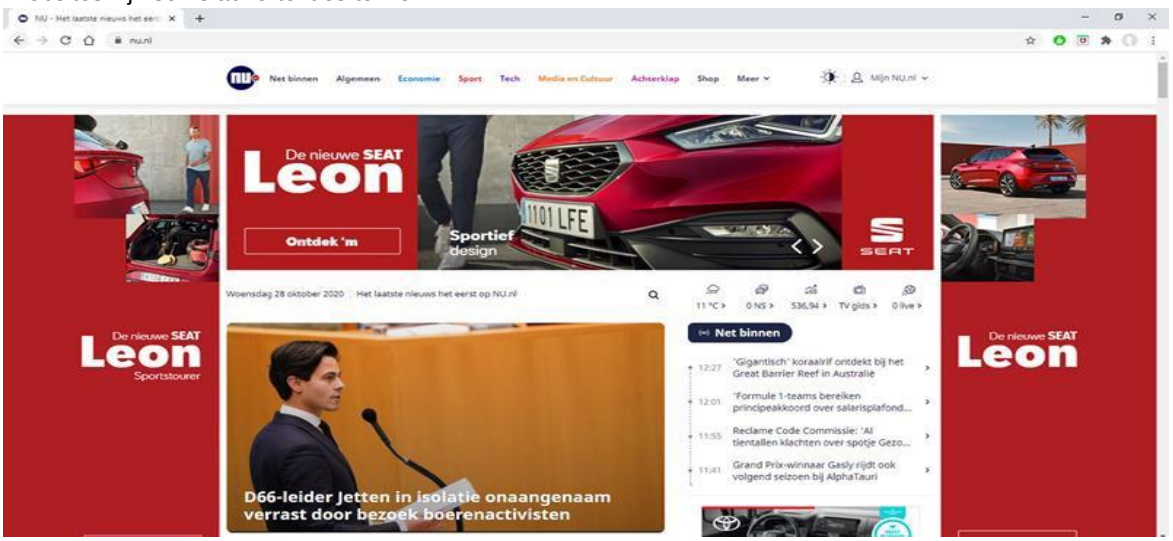
55	**Kan het kwaad wanneer anderen op internet kunnen zien waar ik woon?**
56	**Wat kan er gebeuren als je persoonlijke informatie zoals jouw adres en telefoonnummer via het internet deelt met anderen?**
57	**Deel jij jouw profielgegevens via het internet? Waarom wel/niet?**

ONDERDEEL T	
Profielgegevens zijn openbaar of (voor een deel) verborgen.  	
58	**Is het belangrijk om na te denken over welke profielgegevens je via het internet met anderen deelt?**
59	**Wat kan er gebeuren als de profielgegevens die via het internet worden gedeeld niet meer kloppen?**
60	**Controleer je zo nu en dan of jouw profielgegevens nog wel kloppen?** **Waarom wel/niet?**

ONDERDEEL U	
Met behulp van Social Media worden berichten, foto's en filmpjes met anderen gedeeld.  	
61	**Kunnen mensen met de berichten, foto's en filmpjes die ze van anderen zien controleren wat iemand allemaal heeft gedaan?**
62	**Wat kan er gebeuren als anderen berichten, foto's en filmpjes van jou op het internet zouden tegenkomen?**
63	**Verwijder je zelf wel eens berichtjes, foto's of filmpjes van jezelf van het internet? Waarom wel/niet?**

ONDERDEEL V

Op websites zijn soms advertenties te zien.



64	**Kan iemand weten of de advertenties die je op een website te zien krijgt interessant voor je zijn?**
65	**Wat kan er gebeuren als anderen weten op welke websites ik kom?**
66	**Denk jij als je gaat internetten wel eens na of anderen kunnen zien wat je doet?** **Waarom wel / niet??**

De interviews voor de leraren

GEBRUIKSINSTRUCTIE

Hieronder is kort uitgelegd hoe het interview is opgebouwd en op welke wijze de vragen moeten worden afgenomen.

Voorafgaande aan de afname

- De overdracht van de onderzoeksdocumentatie vindt plaats door middel van een intakegesprek. In het bijzonder worden de procedures van de afname van de vragenlijsten en interviews toegelicht, afnamedata met elkaar afgestemd en overige afspraken gemaakt.
- Bij de leraren van de groepen waarvan de kinderen de vragenlijst krijgen voorgeschoteld wordt een interview afgenomen.
- Het interview bestaat uit 13 vragen die zijn onderverdeeld in 3 categorieën.
- Houd rekening met een maximale afnametijd van een half uur tot 3 kwartier.
- Het interview wordt bij voorkeur individueel afgenomen. Dit kan zowel fysiek op locatie als online.
- Ook wordt het interview in principe digitaal vastgelegd. Dit biedt de interviewer maximale bewegingsruimte tijdens de afname. De aantekeningen en opnamen kunnen dan na afloop worden samengevoegd om te komen tot een zo volledig en zuiver mogelijke dataverzameling.
- Om de betreffende leraren voor te bereiden op de context van het interview worden de vragen al van tevoren gecommuniceerd. Dit heeft als bijkomend voordeel dat tijdens het interview zelf naar alle waarschijnlijkheid sneller en dieper op de inhoud kan worden ingegaan.
- De interviewdata worden geanonimiseerd. Wel wordt gevraagd naar de school, de groep, het aantal kinderen in de groep en het geslacht en de leeftijd van de leraar.
- We vragen expliciet om feedback op het proces van de afname en vernemen dan ook graag hoe het is gelopen, wat wel / niet goed verliep, wat niet duidelijk (genoeg) was, et cetera. Voelt u vrij om mogelijke verbeteringen met ons te delen. Hiertoe is een evaluatieformulier beschikbaar (overdracht tijdens het intakegesprek).

Tijdens de afname

- De interviewvragen worden achter elkaar in de voorgeschreven volgorde gesteld; iedere primaire reactie van de leraar wordt door hem / haar direct daarop daar waar mogelijk voorzien van een beargumenteerde toelichting.
- Net als bij de vragenlijsten benadrukken we het belang van de authenticiteit van de antwoorden: de leraar formuleert zijn / haar eigen antwoorden; de interviewer stelt duidelijke vragen, luistert aandachtig en kritisch en vraagt waar nodig gericht door waarbij suggesties worden vermeden.
- Het eind van het interview wordt in gezamenlijkheid bepaald; als alles is gevraagd en beantwoord wordt er afgerond.

Na de afname

- Alle documentatie wordt verzameld en ingenomen.
- De leraar wordt bedankt voor zijn medewerking (presentje?) en op de hoogte gebracht van de vervolgstappen.

INTERVIEWVRAGEN

ALGEMEEN	
Fijn dat u en uw groep willen participeren in het onderzoek naar Digitale Veiligheid! Voordat we beginnen met het interview willen we eerst enkele algemene gegevens noteren. Alvast bedankt voor het meedoen, we kijken uit naar uw antwoorden!	
01	**Wat is de naam van de school en in welke gemeente is deze gevestigd?**
02	**Welke groep betreft het en hoeveel kinderen zitten er in deze groep?**
03	**Wat is uw geslacht en wat is uw leeftijd?**

BELEID	
Vanuit de overheid wordt aangestuurd op de herziening van de kerndoelen en eindtermen voor het PO en VO. Digitale Geletterdheid is daarbij 1 van de 9 leergebieden die een vaste plek krijgen in het vernieuwde curriculum. Digitale Geletterdheid kent 4 domeinen, te weten: Informatievaardigheden, Mediawijsheid, Computational thinking en ICT-basisvaardigheden. Een belangrijke pijler daarbij is Digitale Veiligheid.	
04	**Is men op uw school op de hoogte van de ontwikkelingen met betrekking tot de herziening van genoemde kerndoelen en eindtermen en die voor Digitale Geletterdheid in het bijzonder? Hoe staat u hier zelf in; wat vindt u ervan?**
05	**Heeft uw school al concreet beleid voor het onderwijs in Digitale Geletterdheid en Digitale Veiligheid in het bijzonder? Hoe manifesteert zich dat? Hoe staat u hier zelf in; wat vindt u ervan?**
06	**Is er op uw school beleid op de scholing van de Digitale Geletterdheid van u en uw collega's? Op welke wijze? Hoe staat u hier zelf in; wat vindt u ervan?**
07	**Is er op uw school beleid op de betrokkenheid van ouders en verzorgers van de kinderen bij het bijbrengen van de Digitale Geletterdheid aan de kinderen? Op welke wijze? Hoe staat u hier zelf in; wat vindt u ervan?**
08	**Hebben op uw school de afgelopen jaren incidenten met betrekking tot Digitale Veiligheid plaatsgevonden? Welke betrof(fen) dit? Is er op uw school specifiek beleid ontwikkeld voor dergelijke incidenten? Waarom wel / niet? Hoe staat u hier zelf in; wat vindt u ervan?**
09	**Van welke ontwikkelingen is er wat betreft Digitale Geletterdheid en Digitale Veiligheid in het bijzonder de komende tijd sprake op uw school? Hoe staat u hier zelf in; wat vindt u ervan?**

ONDERWIJSACTIVITEITEN	
Het belang van de aandacht voor Digitale Veiligheid in de onderwijsactiviteiten kan zich op verschillende manieren manifesteren.	
10	**Is het bijbrengen van Digitale Geletterdheid en Digitale Veiligheid op uw school binnen het huidige reguliere onderwijsprogramma op de een of andere wijze geborgd en zijn er wat dat betreft specifieke aspecten van Digitale Veiligheid te onderscheiden? Waar binnen het onderwijsprogramma en op welke wijze is hier sprake van?**
11	**Welke onderwijsactiviteiten lenen zich volgens u voor om de Digitale Veiligheid van de kinderen te prikkelen en beïnvloeden? Waarom juist deze wel / niet?**
12	**Hebben in uw groep(situatie) de afgelopen jaren incidenten met betrekking tot Digitale Veiligheid plaatsgevonden? Welke betrof(fen) dit? Hoe bent u daar op dat moment mee omgegaan?**
13	**Kunt u de voor u ideale situatie op uw school beschrijven als we het hebben over het bijbrengen van Digitale Veiligheid aan kinderen? Waar bent u wat dat betreft op dit moment al wel en / of juist nog niet tevreden over? Wat moet er wat u betreft nog concreet gebeuren? Heeft u suggesties voor de wijze waarop dat zou kunnen worden geëffectueerd?**

De Cyber Game voor Digitale Veiligheid

INFORMATIE VOORAF

Aangezien de perikelen rondom het Covid19 virus de dataverzameling met behulp van de oorspronkelijke onderzoeksinstrumenten hebben bemoeilijkt, hebben studenten van de opleiding HBO-ICT in opdracht van het lectoraat Cybersecurity & Safety na een gedegen vooronderzoek naar stijl, vorm en inhoud een game voor mobiele Android apparaten ontwikkeld (Bouaali et al., 2018; Oosterwijk et al., 2020) waarmee we een goed toegankelijk en bruikbaar alternatief hebben om leerlingen te bevragen op het gebied van digitale veiligheid.

GEBRUIKSINSTRUCTIE

Het grootste voordeel van deze game schuilt met name in de toegankelijkheid ervan: na installatie kan deze naar verwachting geheel zelfstandig door de leerlingen (en eventueel ook de leraren) worden uitgespeeld. De kanttekening is gelegen in de beperking dat een smartphone of tablet waarop dat daar op Android vereist is. De game is dus niet te spelen op een pc, laptop, Mac, iPhone of iPad.

Een overzicht van de minimale systeemvereisten:

- Een smartphone of tablet met Android (minimale versie 8.0, Oreo) als besturingssysteem
- Een account bij de Google Play Store om de app te kunnen installeren
- De applicatie Google Play Games moet op het apparaat zijn geactiveerd. De app vraagt hier zelf naar overigens tijden de installatie.
- Een Google Play Gamer-ID. Ook deze kan meteen tijdens de installatie van de game zelf worden aangemaakt.

Volg de instructie hieronder om de App genaamd ‘Cyber Game – Digitale Veiligheid’ te installeren:

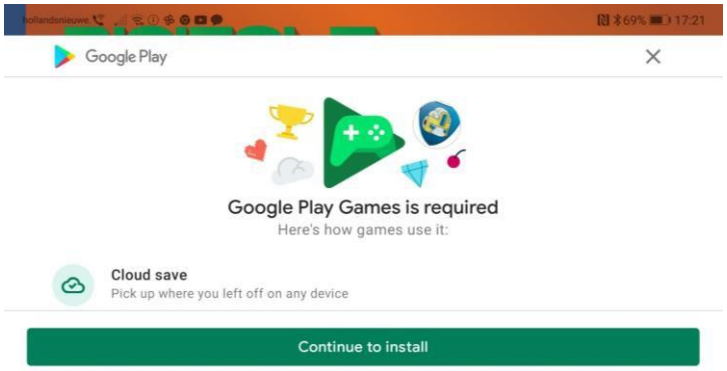
De installatie

Installeer de app vanuit de Google Play Store en start deze nadat de installatie is afgerond.

FIGUUR 1: *De app ‘Cyber Game – Digitale Veiligheid’ in de Google Play Store.*

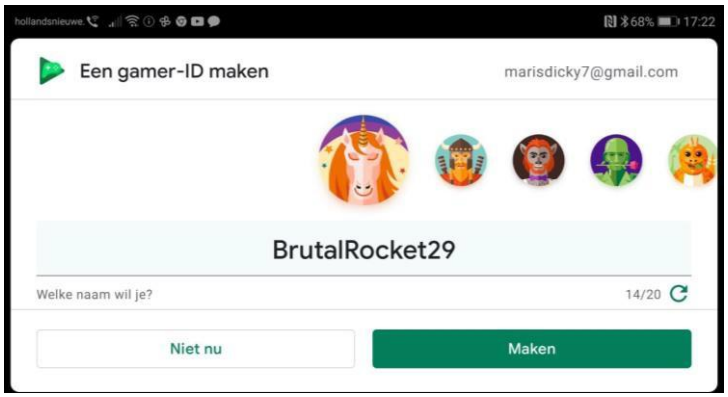
Aangezien de ‘Cyber Game – Digitale Veiligheid app’ onderdeel uitmaakt van het zogenoemde *‘Google Play’* platform, is de installatie van de aanverwante applicatie *‘Google Play Games’* een vereiste om door te kunnen gaan.

Is *'Google Play Games'* nog niet geïnstalleerd, dan zal de volgende melding volgen:



FIGUUR 2: *Er wordt toestemming gevraagd om de verplichte app 'Google Play Games' te installeren.*

Binnen het *'Google Play'* platform geldt bovendien als voorwaarde dat een *'Gamer-ID'* benodigd is. Indien geen geldig 'Gamer-ID' wordt aangetroffen, volgt de melding om dit alsnog te doen:



FIGUUR 3: *Er wordt gevraagd een 'Gamer-ID' te maken waarbij het mogelijk is zelf een geschikte naam in te geven.*

Let op: Kies bij voorkeur een *'Gamer-ID'* dat geheel los staat van en niet terug te herleiden is naar jouw eigen (echte) naam!

Het spel

Kies voor *'Nieuw begin'* om het spel te starten. Het is de bedoeling dat het spel helemaal wordt uitgespeeld. Wanneer dat is gelukt, volgt nog het ultieme *'Eindgevecht'* dat bestaat uit 20 kennisvragen die moeten worden beantwoord. Deze antwoorden worden automatisch opgeslagen in een database waar alleen de onderzoekers toegang toe hebben; zij kunnen de resultaten in het kader van het onderzoek raadplegen en analyseren.

FIGUUR 4: Het startscherm van het spel.

In het spel moet de hoofdrolspeler Simon, een robot, zien te ontsnappen uit een vijf verschillende ruimtes. Dat doet hij door sleutels te zoeken en de vragen die daarbij horen te beantwoorden. Voor elke juist beantwoorde vraag ontvangt Simon een letter. Zodra alle letters verzameld zijn kan hij de deur van de ruimte openen om de volgende ruimte binnen te gaan. Bovendien kan Simon tijdens zijn zoektocht ook muntjes verzamelen waarmee hij zijn score verhoogt.

FIGUUR 5: Robot Simon in een van de ruimtes.

De vragen in het spel zijn gerelateerd aan de leerplankaders van het (SLO, 2018) aan de hand waarvan leraren, lerarenopleiders, vakdidactici, (curriculum)experts en scholen in opdracht van de overheid onder de noemer *curriculum.nu* samen verder werken aan de herziening van het landelijk curriculum voor primair en voortgezet onderwijs. Het betreft voornamelijk kennisgerichte meerkeuzevragen. Reken op een half uur tot drie kwartier om het spel volledig uit te kunnen spelen.

FIGUUR 6: Voorbeeld van een vraag tijdens het spel.

Literatuur

De resultaten

Zoals eerder aangegeven worden de antwoorden op de kennisvragen uit het *'Eindgevecht'* automatisch opgeslagen in een database waar alleen de onderzoekers toegang toe hebben. De resultaten zijn geanonimiseerd en niet meer te herleiden naar een individuele leerling (aangenomen dat er een fictieve gamerID is opgegeven).

Literatuurlijst

Bouaali, S., Alghazouli, W., Kouwenhoven, S., Elswijk, H. van, & Oude, I. den. (2018). *Onderzoek kennisoverdracht voor de applicatie Digitale Veiligheid*.

Curriculum.nu. (2018). *Curriculum.nu. Digitale geletterdheid uitgewerkt in digitale vaardigheden*.

Hevner, R., March, S., & Park, J. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75– 105.

Janssens, J. M. A. M. (1998). *Ogen doen onderzoek* (Pearson Benelux B.V. (ed.); 10th ed.).

Oosterwijk, J. van, Remon, T., Yanoah, W., & Yunus, G. (2020). *Cyber Game Eindverslag*.

SLO. (2018). *Curriculum van de toekomst, leerlijnen digitale geletterheid*.

van der Grient, R., Schippers, N., & Kevin, H. (2020). *Veilig Online 2020*.