

Digitale veiligheid van digibeten

In hoeverre wordt digitale veiligheid meegenomen in de cursussen voor digibeten?

1



Lectoraat Cybersecurity & Safety
2020

¹ Digitaleoverheid.nl
let's change
YOU. US. THE WORLD.

DE HAAGSE
HOGESCHOOL

Digitale veiligheid van digibeten

In hoeverre wordt digitale veiligheid meegenomen in de cursussen voor digibeten?

Auteurs

L.C. de Kok (l.c.dekok@hhs.nl)

M.E.M. Spruit (m.e.m.spruit@hhs.nl)
cybersecurity@hhs.nl

Lectoraat

Lectoraat Cybersecurity & Safety

Datum

29 september 2020

Type project

Evaluatierapportage in opdracht van gemeente Dordrecht en Stichting Lezen & Schrijven

Versie

Definitief 1.0

De Haagse Hogeschool, 2020

Digitale veiligheid van digibeten

Lectoraat Cybersecurity & Safety – versie Definitief 1.0
De Haagse Hogeschool, 2020

Inhoudsopgave

1	Inleiding	4
2	Methode	5
3	Resultaten.....	6
3.1	Cursus 1. Ook Digitaal! (Instroomniveau).....	6
3.1.1	Digitale Veiligheidsonderdelen	6
3.1.2	Ontbrekende onderdelen	6
3.2	Cursus 2. Succes! Digitale Vaardigheden (Basisniveau 1)	7
3.2.1	Digitale Veiligheidsonderdelen	7
3.2.2	Invulling opdrachten.....	7
3.2.3	Ontbrekende onderdelen	8
3.3	Digitaalkaarten (Instroom 0 en Basisniveau 1).....	8
3.4	Cursus 3. Klik & Tik (Basisniveau 2)	9
3.4.1	Digitale Veiligheidsonderdelen	9
3.4.2	Invulling opdrachten.....	9
3.4.3	Ontbrekende onderdelen	10
4	Conclusie en aanbevelingen	11
	Literatuurlijst.....	12
	Bijlage 1. Baseline Digitale Veiligheidskennis- en vaardigheidsleerdoelen.....	13
	Bijlage 2. Curriculum.nu leerdoelen	16

1 Inleiding

Digitale geletterdheid is niet alleen een kwestie van kennis over digitale technologie, maar ook van vaardigheden met betrekking tot het omgaan met deze technologie. In Nederland heeft 22% van de bevolking van 12 jaar en ouder geen of weinig ICT-vaardigheden en zijn daarom digitaal laaggeletterd te noemen (CBS, 2016). Als deze groep zich op internet begeeft, is het belangrijk dat er veilig gebruik wordt gemaakt van deze technologie. Digitale veiligheid bevat verschillende componenten. Denk hierbij bijvoorbeeld aan het herkennen van veilige en onveilige websites, phishing, goed omgaan met wachtwoorden en borgen van iemands privacy. Stichting Lezen & Schrijven en oefenen.nl hebben verschillende cursussen ontwikkeld voor digitaal laaggeletterden (digibeten). Digitale veiligheid is een onderdeel van dit cursusaanbod.

In dit onderzoeksrapport wordt gepresenteerd in hoeverre de cursussen voor digibeten de digitale veiligheidselementen bevatten. Dit gebeurt aan de hand van een baseline digitale veiligheidskennis- en vaardigheden die is opgesteld door onderzoekers van het lectoraat Cybersecurity & Safety van De Haagse Hogeschool. De centrale onderzoeksvraag van dit onderzoek is als volgt:

In hoeverre wordt digitale veiligheid meegenomen in de cursussen voor digibeten?

De cursussen van Stichting Lezen & Schrijven (Ook Digitaal! en Succes! Digitale Vaardigheden) en oefenen.nl (Klik & Tik) voor digibeten die worden getoetst zijn:

1. Ook Digitaal (Instroomniveau 0)
2. Succes! Digitale vaardigheden (Basisniveau 1)
3. Klik & Tik (Basisniveau 2).

Aanvullend aan de cursussen Ook Digitaal! En Succes Digitale Vaardigheden zijn Digitaalkaarten ontwikkeld. Deze digitale kaarten dienen als naslagwerk voor de deelnemers als zij de cursus gevolgd hebben. De cursussen en Digitaalkaarten worden getoetst aan een baseline van digitale veiligheidskennis- en vaardigheidsleerdoelen op drie niveaus.

Het onderzoek wordt uitgevoerd in opdracht van gemeente Dordrecht in het kader van het project digitale weerbaarheid voor digibeten. In hoofdstuk 2 kan u lezen wat de onderzoeksmethode is geweest. In hoofdstuk 3 zullen de resultaten worden besproken. In hoofdstuk 4 worden de conclusies en aanbevelingen gepresenteerd.

2 Methode

In dit hoofdstuk wordt besproken hoe het onderzoek is uitgevoerd. Doel van dit onderzoek is om erachter te komen in hoeverre de cursussen voor digibeten van Stichting Lezen & Schrijven en oefenen.nl digitale veiligheid meenemen. Om de cursussen te toetsen is een baseline digitale veiligheidskennis- en vaardighedenleerdoelen door de onderzoekers van de Haagse Hogeschool ontwikkeld (Bijlage 1). De kennis- en vaardigheidsdoelen van digitale veiligheid zijn afgeleid uit de leerdoelenlijst van Curriculum.nu (Bijlage 2)². Curriculum.nu is de landelijke organisatie die wettelijke leerdoelen vastlegt voor het onderwijs. In die hoedanigheid hebben zij ook leerdoelen vastgelegd voor digitale veiligheid. Curriculum.nu maakt onderscheid in een drietal niveaus: onderbouw lager onderwijs, bovenbouw en lager onderwijs en onderbouw voortgezet onderwijs. Deze drie niveaus zijn in lijn gebracht met de drie niveaus van Stichting Lezen & Schrijven: instroomniveau, basisniveau 1 en basisniveau 2. In totaal zijn er 15 kennisleerdoelen en 13 vaardigheidsleerdoelen verdeeld over drie niveaus. Zie Tabel 1 voor de aansluiting van de baseline en de cursussen.

De onderzoekers van De Haagse Hogeschool hebben de leerdoelen van Curriculum.nu als uitgangspunt genomen en van enkele aanpassingen voorzien met inachtneming van het huidige niveau van deze doelgroep en de relevantie op hun dagelijkse gebruik. De toepasselijkheid van de baseline is besproken en aangepast in overleg met de cursus-ontwikkelaar van Stichting Lezen & Schrijven. Daarnaast is de baseline besproken met twee digitale veiligheidsexperts op inhoudelijke volledigheid en volgorde van de leerdoelen.

Om te borgen dat alle inhoudelijke elementen voldoende zijn meegenomen in de leerdoelen is de verdeling van Veiliginternetten.nl gebruikt. Deze website heeft een onderverdeling in thema en basisbeveiliging. Veilig internetten is een website van de centrale overheid waar mensen tips, tricks en praktisch stap voor stap uitleg kunnen vinden over wat zij kunnen doen en laten om veilig te internetten.³ De volgende basisbeveiliging en thema's zijn niet meegenomen omdat deze niet relevant zijn voor deze doelgroep en/of op een ander onderwerp zijn meegenomen: Veilig op reis, Internet of Things Je bedrijf en Kinderen Online. Het resultaat van de baseline die gebruikt zal worden bij de evaluatie is te vinden in Bijlage 1.

De inhoud van de drie cursussen en de Digitaalkaarten zijn geheel bekeken waar en hoe onderdelen van digitale veiligheid zijn besproken. Deze zijn in een spreadsheet gedocumenteerd en naast de leerdoelen gelegd. Bij interesse kan de data van de resultaten opgevraagd worden bij de onderzoekers. De resultaten hiervan worden in het volgende hoofdstuk besproken.

Niveau Cursus	Cursus Stichting Lezen & Schrijven en oefenen.nl
Instroomniveau 0 (onderbouw lager onderwijs)	Ook Digitaal!
Basisniveau 1 (bovenbouw lager onderwijs)	Succes! Digitale Vaardigheden
Basisniveau 2 (onderbouw voortgezet onderwijs)	Klik & Tik

Tabel 1. Onderverdeling en aansluiting niveaus cursussen en baseline

² Curriculum.nu (2019). <https://www.curriculum.nu/download/voorstellen-digitale-geletterdheid/>

³ <https://veiliginternetten.nl/>

3 Resultaten

In dit hoofdstuk staan de resultaten van de toetsing van de drie cursussen van Stichting Lezen & Schrijven aan de ontwikkelde baseline digitale veiligheid. Hier wordt besproken welke digitale veiligheids-leerdoelen worden meegenomen en welke ontbreken in de cursussen. De cursussen zijn vraaggericht. Dit kan als effect hebben dat de ene deelnemer een onderdeel uitgebreider behandelt dan een ander. In de resultaten wordt ervan uitgegaan dat alle onderdelen worden behandeld. In de resultaten wordt voor elke cursus weergegeven of de besproken onderwerpen op dezelfde niveaus zijn belegd. Verder wordt gepresenteerd of de invulling van de opdrachten in lijn zijn met de digitale veiligheidsrichtlijnen. Ten slotte wordt weergegeven waar de cursus niet aansluit op de baseline.

3.1 Cursus 1. Ook Digitaal! (Instroomniveau)

Stichting Lezen & Schrijven heeft de cursus Ook Digitaal! ontwikkeld vanuit de vraag naar cursusmateriaal voor digitale vaardigheden op het instroomniveau, aansluitend bij de leervragen en wensen van digibeten. Deze cursus richt zich op mensen met lage digitale vaardigheden die ook laaggeletterd zijn. In Ook Digitaal! verbeteren zij hun digitale vaardigheden. Het is de eerste cursus van drie die digibeten kunnen volgen.

3.1.1 Digitale Veiligheidsonderdelen

In deze cursus nemen de deelnemers de volgende digitale veiligheids-kennis en -vaardigheden tot zich. Tussen haakjes staat bij welk kennis- of vaardigheidsdoel het aansluit.

- o Informatie en accounts zijn af te schermen met wachtwoorden, hier dient vertrouwelijk mee om te worden gegaan. (K0.1, K0.2)
- o Veilige en minder veilige websites kunnen onderscheiden worden door middel van het checken van een slotje en/of https://. (K1.1, V1.1)
- o Wat cookies zijn en wat de functie ervan is. (K1.2)
- o Informatie op internet blijft hier op staan en is niet makkelijk te wissen. Daarom dient persoonlijke informatie niet met iedereen gedeeld te worden. (K0.3, K1.4, V1.3)

Zoals te zien in bovenstaande punten is dit een instap-cursus en worden een aantal digitale veiligheidsaspecten op een eenvoudige manier gepresenteerd. Dit is grotendeels in lijn met de opgestelde baseline. Digitale veiligheidsaspecten zoals verschillende dreigingen (identiteitsfraude, phishing, openbare WiFi) en cybercrime maatregelen (virusscanners, updates, maken van sterke wachtwoorden, back-ups) worden hier (nog) niet behandeld. Er zijn geen specifieke aandachtspunten met betrekking tot de invulling van de opdrachten.

In Tabel 2 is te zien welke leerdoelen wel en niet behandeld worden in Ook Digitaal! De groene kleur geeft aan dat het behandelde in lijn is met de baseline. Geel geeft aan dat er ook onderdelen worden behandeld die bij een hoger niveau horen. De rode kleur geeft aan dat onderdelen niet worden behandeld die wel bij dit niveau horen.

3.1.2 Ontbrekende onderdelen

Het is in lijn met de baseline dat de meeste punten, die hierboven zijn genoemd, niet in deze cursus zijn meegenomen. Toetsend aan de baseline, ontbreken namelijk twee onderdelen in de cursus:

- o Deelnemers kunnen uitleggen welke hulp ze kunnen inschakelen als ze een digitaal incident of een vraag hebben (K0.4)
- o Deelnemers weten hoe ze een sterk wachtwoord kunnen bedenken (V0.1).

	Ook Digitaal! (Instroomniveau)	
	Kennis	Vaardigheden
Wordt behandeld huidig niveau	K0.1 t/m 0.3	n.v.t.
Wordt behandeld hoger niveau	K1.1, K1.2, K1.4	V1.1, V1.3
Ontbreekt huidig of onderliggend niveau	K0.4	V0.1

Tabel 2. Toetsing kennis- en vaardigheidsleerdoelen Ook Digitaal!

3.2 Cursus 2. Succes! Digitale Vaardigheden (Basisniveau 1)

De lesmethode Succes! Digitale vaardigheden is de opvolger van Ook Digitaal!. Succes! is een lesmethode voor volwassenen die beter willen leren lezen, schrijven en rekenen. Deze cursus richt zich op mensen met lage digitale vaardigheden die ook laaggeletterd zijn. Situaties uit het dagelijks leven en de werkomgeving, zoals het regelen van bankzaken, staan hierin centraal. Er is Succes!-materiaal over digitale onderwerpen, zoals 'Kopen op internet' en 'Wat doe jij op het internet?'.

3.2.1 Digitale Veiligheidsonderdelen

In deze cursus nemen de deelnemers de volgende digitale veiligheidskennis en vaardigheden tot zich:

- o Wat phishing / spam is en hoe je ermee om moet gaan (K1.3, V1.2)
- o Opslaan en verwijderen van bestanden (randvoorwaarde, V2.1, V2.4)
- o Dat het belangrijk is bij online winkelen om een bekende, betrouwbare site te kiezen (V2.7)
- o Wat (sterke) wachtwoorden zijn en hoe je deze kan onthouden (K0.1, V0.1, V1.5)
- o Belang van uitloggen op openbare computers (K0.2)

Qua omvang is dit een kleinere cursus ten opzichte van Ook Digitaal!. Het digitale veiligheidscomponent komt hier minder naar voren en er is meer aandacht voor andere digitale vaardigheden. In deze cursus is geen (uitgebreide) aandacht voor het belang van privacy online en omgang met sociale media (K0.3, K1.4, V1.3, V1.4), het inschakelen van hulp bij een (mogelijk) incident (K0.4), de verschillende vormen van cybercrime en gevaar van downloaden en apps (K1.5).

3.2.2 Invulling opdrachten

In een aantal opdrachten in deze cursus kan het digitale veiligheidsaspect completer en/of meer in lijn met de digitale veiligheidsrichtlijnen gepresenteerd worden. Hieronder een korte toelichting:

- o In een opdracht wordt kort besproken wat phishing/spam is en wordt dit benoemd als 'ongewenste e-mails' en "reclame" (Basis1 D2 Opdracht 7). Hier wordt niet genoemd hoe een dergelijke mail kan worden herkend en dat dit een phishing-mail kan zijn.
- o In een voorbeeld van een smartphone-ontgrendeling gebruikt iemand de letter van zijn voornaam (IND1, 1B). Het is geen veilige optie om een wachtwoord te relateren aan persoonsgegevens.
- o Wanneer WhatsApp-groepen worden besproken, wordt een voorbeeld gegeven dat iemand op vakantie gaat en dit deelt met zijn burens (Basis1 D1). Hier wordt niet genoemd dat dit een vertrouwde omgeving is, maar dat dit soort informatie bijvoorbeeld beter niet op sociale media met iedereen gedeeld kan worden.
- o Bij de bespreking van het herkennen van veilige websites, wordt met name gestuurd op het slotje en enigszins of het een bekende website is (D3, Opdr7A). Aanvullend zou kunnen worden gekeken naar erkende certificaten van webshops.

3.2.3 Ontbrekende onderdelen

In lijn met de gestelde baseline van kennis- en vaardigheidsniveau 1 zou niveau 1 van de baseline in totaal gehaald moeten worden. Sommige punten van niveau 1 zijn al meegenomen in Ook Digitaal! (niveau 0) en hoeven dus niet in de tweede cursus nogmaals worden behandeld, al geeft herhaling wel de mate van urgentie aan en blijft de kennis beter hangen.

Drie leerdoelen zijn nog niet behandeld in Ook Digitaal! En Succes Digitale Vaardigheden van niveau 0 en 1. De volgende ontbreken:

- o Het inschakelen van hulp bij een digitaal incident (K0.4)
- o Het uitleggen dat op het oog gratis digitale middelen en diensten meestal niet 'gratis' zijn en je hier iets voor inlevert (K1.5)
- o Een gedegen afweging moet worden gemaakt welke informatie wordt gedeeld, aansluitend bijvoorbeeld bij de WhatsApp-opdracht met de burens (V1.4).

Voor de herhaling zou het goed zijn om uit te leggen wat persoonsgegevens zijn en wat de waarde daarvan is (K0.3, K1.4, V1.3), dat er veilige en mindere veilige websites bestaan en dat de deelnemer deze kan herkennen (K1.1, V1.1). Cookies (K21.2) hoeven niet nogmaals te worden besproken omdat dit onderwerp in Ook Digitaal! al uitgebreid aan bod is gekomen.

	Succes! Digitale Vaardigheden (Basisniveau 1)	
	Kennis	Vaardigheden
Wordt behandeld huidig niveau	K0.1, K0.2, K1.3	V0.1, V1.2, V1.5
Wordt behandeld hoger niveau	K2.1, K2.2	V2.1, V2.4, V2.7
Ontbreekt huidig of onderliggend niveau	K0.3, K0.4, K1.1, K1.2, K1.4, K1.5	V1.1, V1.3, V1.4

Tabel 3. Toetsing kennis- en vaardigheidsleerdoelen in Succes! Digitale Vaardigheden

3.3 Digitaalkaarten (Instroom 0 en Basisniveau 1)

Aanvullend aan de eerste twee cursussen zijn ook "Digitaalkaarten" ontwikkeld met uitgebreidere uitleg van de verschillende digitale vaardigheden. De Digitaalkaarten worden aan de deelnemers meegegeven als het onderdeel behandeld is, zodat de deelnemers het nog eens kunnen opzoeken, nalezen en mogelijk toepassen. Omdat beide cursussen vraaggestuurd zijn, kan het zijn dat niet alle Digitaalkaarten worden behandeld. Deze kaarten zijn onderverdeeld in Instroomniveau 0 en Basisniveau 1 en sluiten daarom aan bij de cursus Ook Digitaal! en Succes!.

	Instroomniveau (Ook Digitaal!)		Basisniveau 1 (Succes!)	
	Kennis	Vaardigheden	Kennis	Vaardigheden
Wordt behandeld huidig niveau	0.1	-	0.1 t/m 0.4 1.1 t/m 1.4	0.1
Wordt behandeld hoger niveau	1.1, 1.2, 1.4	1.1, 1.3, 1.4 2.7 (3 x)	2.1 t/m 2.5	1.5, 2.1, 2.6, 2.7
Ontbreekt huidig of onderliggend niveau	0.2 t/m 0.4	0.1	1.5	1.1

Tabel 4. Toetsing kennis- en vaardigheidsleerdoelen voor Digitaalkaarten van instroomniveau en Basisniveau 1.

Bij het instroomniveau ontbreekt:

- o Uitleggen waar eigen gegevens en bestanden zijn opgeslagen, wat persoonsgegevens zijn, hulp inschakelen. Deze worden echter wel behandeld bij basisniveau 1. (K0.2 t/m 0.4)

- o Bedenken en onthouden van sterke wachtwoorden. Ook deze wordt behandeld bij basisniveau 1. (V 0.1)

Bij het basisniveau ontbreekt:

- o Kan uitleggen waarom op het oog gratis digitale middelen en diensten meestal niet gratis zijn. (K1.5)
- o Veilige en onveilige websites herkennen. Dit wordt wel behandeld bij het instroomniveau. (V1.1)

3.4 Cursus 3. Klik & Tik (Basisniveau 2)

In de Klik & Tik cursussen van oefenen.nl krijgen deelnemers meer durf en leren zij basale computervaardigheden die zij ook daadwerkelijk (gaan) gebruiken. Het is de cursus opvolgend aan Succes! Digitale Vaardigheden.

In Tabel 5 is te zien welke kennis- en vaardigheidsleerdoelen zijn meegenomen. Omdat de meeste onderwerpen meerdere keren zijn meegenomen is ditmaal ook de frequentie benoemd van de leerdoelen.

	Klik & Tik (Basisniveau 2)	
	Kennis	Vaardigheden
Wordt behandeld huidig niveau	2.1 (7x), 2.2 (4x), 2.3 (1x), 2.4 (1x), 2.5 (2x)	2.1 (1x), 2.2 (2x) 2.3 (2x) 2.6 (5x) 2.7 (2x)
Wordt behandeld lager niveau	0.1 (4x) 0.3 (3x) 0.4 (4x) 1.1 (1x) 1.2 (4x), 1.3 (1x), 1.4 (3x) 1.5 (2x)	0.1 (4x) 1.1 (4x) 1.2 (5x) 1.3 (1x) 1.4 (2x) 1.5 (4x),
Ontbreekt huidig niveau	2.6	2.4 & 2.5
Ontbreekt lager niveau	0.2	-

Tabel 5. Toetsing kennis- en vaardigheidsleerdoelen in Klik & Tik (Basisniveau 2)

3.4.1 Digitale Veiligheidsonderdelen

In deze cursus nemen de deelnemers de volgende digitale veiligheidskennis en -vaardigheden tot zich:

- o Bewust gebruik van openbare Wifi (niet genoemd in leerdoelen)
- o Maken, onthouden en gebruiken van sterke wachtwoorden (V1.5)
- o Veilig gebruik van internetbankieren en online winkelen (V2.6, V2.7)
- o Bewuste afweging welke informatie op sociale media (Facebook) wordt gedeeld (K2.2, K2.3, K2.4)
- o Aandacht voor weerbaarheid: wat de deelnemer moet doen als hij vervelende berichten krijgt, spam of cookies, dat een virusscanner gebruikt kan worden, twee e-mailadressen kunnen worden gebruikt en dat belangrijke informatie zoals DigiD nooit gedeeld moet worden via internet. (K2.1)
- o Aanpassen van privacy-instellingen bij het downloaden van apps (V2.1, V2.2, V2.3)
- o De deelnemer raakt bekend met verschillende gevaren zoals phishing en (ongewenste)reclame (K2.2)

3.4.2 Invulling opdrachten

Op blz. 6 van de cursus wordt geadviseerd het wachtwoord van oefenen.nl op te schrijven. Dat is geen veilig advies, omdat de cursist mogelijk dit wachtwoord vaker gebruikt en het niet een veilige plek is om het wachtwoord te bewaren. In de opdrachten worden verder geen onveilige adviezen gegeven.

3.4.3 Ontbrekende onderdelen

In lijn met de gestelde baseline van kennis- en vaardigheidsniveau 2 zou niveau 2 van de baseline in totaal gehaald moeten worden. Het gaat om de volgende punten:

- o Kan uitleggen wat updates zijn en het nut ervan uitleggen (K 2.6).
- o Een reservekopie c.q. back-up van de gegevens en bestanden maken en deze weer terughalen (V 2.4)
- o Kunnen uitvoeren van een update en/of weten hoe dit automatisch gebeurt (V 2.5)

Hieruit komt naar voren dat in geen van de cursussen aandacht is voor back-ups en updates. Echter zijn er ook zaken behandeld die in eerste instantie niet in de leerdoelen meegenomen waren. Zoals:

- o Het bewust gebruiken van onversleutelde WiFi
- o Aanmoedigen van aanschaffen van virusscanners
- o Nemen van twee e-mailadressen, zodat reclame naar het tweede e-mailadres gestuurd kan worden.

4 Conclusie en aanbevelingen

In dit hoofdstuk zullen de conclusies van de resultaten worden belicht. Hierna zullen enkele aanbevelingen gedaan worden ter verbetering van de cursussen voor digibeten.

Over het algemeen kan geconcludeerd worden dat de meeste digitale veiligheidsonderdelen in de cursussen worden behandeld. Daarnaast lagen de baseline en het aanbod in de cursussen qua niveau meestal op dezelfde lijn. Discrepancie bestaat wel in de cursus Ook Digitaal! En Succes! Digitale Vaardigheden. Veel leerdoelen van de baseline die op basisniveau 1 staan, worden al bij de eerste cursus behandeld (instroomniveau 0). Het is daarentegen beter dat het al in de eerste cursus wordt behandeld, die waarschijnlijk meer mensen volgen, dan pas in de tweede cursus. Er kan overwogen worden het gewicht van digitale veiligheid iets meer te verdelen over de twee cursussen.

In de eerste cursus Ook Digitaal! ontbreekt het vragen van hulp bij een incident of vraag, en het bedenken van een sterk wachtwoord. Het vragen van hulp wordt ook niet bij de tweede cursus Succes! Digitale Vaardigheden behandeld. Hier ontbreekt eveneens het risico tot een inbreuk op de privacy bij het downloaden van 'gratis' apps en het delen van informatie via sociale media. Bij DigitaalKaarten, die als naslagwerk dienen van de eerste twee cursussen, worden de volgende kennisdoelen niet meegenomen: uitleggen waar eigen gegeven en bestanden zijn opgeslagen, wat persoonsgegevens zijn en het inschakelen van hulp. Eveneens wordt de vaardigheid niet behandeld hoe een sterk wachtwoord kan worden bedacht en onthouden. Bij de laatste cursus, Klik & Tik, wordt de kennis en vaardigheid niet bijgebracht van het belang en het uitvoeren van een update. Daarnaast worden de vaardigheden niet geleerd hoe een back-up kan worden gemaakt.

In de resultaten zijn ook een aantal voorbeelden genoemd waarbij de invulling van de opdracht niet aansluit bij de richtlijn van digitale veiligheid. Hier zou nog eens naar gekeken kunnen worden.

In zijn totaliteit, van de 15 kennisdoelen en 13 vaardigheidsdoelen, zijn dit slechts enkele aandachtspunten die ontbreken in het cursusaanbod. Het belangrijkste dat ontbreekt is dat er geen aandacht is voor updates en back-ups. Dit zijn effectieve maatregelen waar de digitale veiligheid in grote mate kan worden versterkt. In het cursusaanbod worden echter ook aanbevelingen gedaan die belangrijk zijn, maar die initieel niet in de baseline worden behandeld. Dit zijn respectievelijk het bewust gebruiken van onversleutelde WiFi, het gebruik van virusscanners en het nemen van twee e-mailadressen. Met name die eerste twee, zouden ook als leerdoel geformuleerd moeten worden.

Uit deze conclusies volgen een aantal aanbevelingen:

- o Overwogen kan worden het aantal digitale veiligheidsonderdelen eerlijker te verdelen over Ook Digitaal! En Succes!
- o Alle ontbrekende leerdoelen op het desbetreffende niveau toevoegen
- o In de resultaten is gebleken dat enkele invullingen van opdrachten niet voldoen aan de digitale veiligheidsrichtlijnen. Er wordt geadviseerd hier nog eens naar te kijken en waar mogelijk aan te passen.
- o Updaten en het maken van back-ups meenemen in het cursusaanbod
- o Aan de baseline digitale veiligheid toevoegen: "het bewust gebruiken van onversleutelde WiFi" en "het gebruik van virusscanners".

Literatuurlijst

CBS (2016) – ICT-vaardigheden van Nederlanders. <https://www.cbs.nl/nl-nl/achtergrond/2016/30/ict-vaardigheden-van-nederlanders> (september 2020)

Curriculum.nu – Digitale Geletterdheid. <https://www.curriculum.nu/download/voorstellen-digitale-geletterdheid/> (juli 2020)

Digitale overheid www.digitaleoverheid.nl (augustus 2020)

Klik & Tik werkboek, ISBN 978-90-8696-494-9

Klik & Tik werkboek De Tablet (Android), ISBN 978 90 86 96 344 7

Ook Digitaal! cursuspakket Stichting Lezen & Schrijven

Succes! Digitale Vaardigheden cursuspakket Stichting Lezen & Schrijven

Veilig Internetten, <https://veiliginternetten.nl/> (juli 2020)

Bijlage 1. Baseline Digitale Veiligheidskennis- en vaardigheidsleerdoelen

De leerdoelen zijn onderverdeeld in basisbeveiliging en thema's, in lijn met de onderverdeling van veiliginternetten.nl. IoT, en Veilig op reis zijn niet meegenomen uit basisbeveiliging. IoT is te geavanceerd voor deze doelgroep en Veilig op reis valt ook onder de andere vormen van Basisbeveiligingen. Bij de thema's is incidenten toegevoegd omdat dit een reactieve maatregel is in plaats van een preventieve. "Je bedrijf" en "kinderen online" zijn uit de selectie gelaten omdat deze niet relevant is voor deze doelgroep. De labels tussen haakjes verwijzen naar de lijst van Curriculum.nu.

Randvoorwaarden voor het voldoen aan de volgende leerdoelen zijn de volgende zaken:

Instroomniveau 0:

- Kan uitleggen wat een account op een computer is en waar je die voor nodig hebt.
- Kan mappen aanmaken en de eigen gegevens en bestanden in mappen opslaan, verplaatsen en terugvinden.
- Kan gegevens en bestanden op een computer die niet meer nodig zijn opruimen.
- Kan eenvoudige computerhandelingen uitvoeren zoals opstarten, inloggen.

Basisniveau 1:

- Kan een account maken

<i>Kennis op het gebied van veilig gebruik van digitale technologie</i>			
		Basisbeveiliging	Thema
Instroom-niveau: onderbouw lager onderwijs	K0.1 Kan uitleggen dat accounts beveiligd zijn met wachtwoorden o.i.d. en hoe ze daar verstandig mee om kunnen gaan (1.2).	Wachtwoorden	Sociale Media, Internetbankieren, Online Winkelen
	K0.2 Kan uitleggen waar de eigen gegevens en bestanden zijn opgeslagen en hoe deze toegankelijk zijn.	- Algemeen - Back-up	N.v.t.
	K0.3 Kan uitleggen wat persoonlijke gegevens zijn en dat je die beter niet met iedereen kan delen (1.5).	N.v.t.	Privacy Sociale Media
	K0.4 Kan uitleggen welke hulp je kan inschakelen als je een digitaal incident of vraag hebt (1.8).		Incidenten
Basisniveau 1: bovenbouw lager onderwijs	K1.1 Kan uitleggen dat er veilige en minder veilige websites bestaan en hoe je die kan herkennen (1.1).	Cybercrime	Online Winkelen
	K1.2 Kan uitleggen wat cookies op het internet zijn en hoe je daar mee om kan gaan.	N.v.t.	Privacy
	K1.3 Kan uitleggen waarom je beter niet op een koppeling kan klikken als je de bron niet kent en vertrouwt	- Cybercrime - Nepmail of neptelefoontje	N.v.t.
	K1.4 Kan uitleggen welke waarde persoonsgegevens hebben voor jezelf en voor anderen en dat daarbij verschillende belangen kunnen spelen (2.7).	- Cybercrime	Privacy Sociale Media
	K1.5 Kan uitleggen waarom op het oog gratis digitale middelen en diensten meestal niet gratis zijn (2.5).	- Downloaden - Apps	Privacy

Basisniveau 2: onderbouw voortgezet onderwijs	K2.1 Kan de belangrijkste gevaren van digitale technologie uitleggen, zoals malware, virussen, hacking, phishing (social engineering) en spam.	- Cybercrime - Nepmail / telefoontje - Virus	Draadloos Internet Internetbankieren
	K2.2 Kan uitleggen hoe het internet misbruikt kan worden, bijvoorbeeld voor illegaal downloaden en verspreiden van persoonlijke informatie.	- Cybercrime - Downloaden	Sociale Media
	K2.3 Kan uitleggen welke sporen je achter kan laten op het internet en hoe je daar rekening mee kan houden (1.6, 2.9).		Privacy
	K2.4 Kan uitleggen dat "eens op internet, altijd op internet" (2.10).		Privacy
	K2.5 Kan uitleggen welke nadelen er aan het gebruik van sociale media kunnen kleven.		Sociale Media
	K2.6 Kan uitleggen wat updates zijn en het nut ervan	Updates	
Vaardigheden op het gebied van veilig gebruik van digitale technologie			
		Basis beveiliging	Thema
Instroom-niveau: onderbouw lager onderwijs	V0.1 Kan een sterk wachtwoord bedenken en onthouden.		
Basisniveau 1: bovenbouw lager onderwijs	V1.1 Kan een veilige of onveilige website herkennen	Cybercrime Downloaden Updaten	
	V1.2 Kan een eenvoudige phishing-mail herkennen en weggooien.	Nepmail of telefoontje	
	V1.3 Kan persoonsgegevens en andere waardevolle gegevens herkennen en daarnaar handelen (2.11).		Privacy
	V1.4 Kan een gedegen afweging maken over welke gegevens, foto's, filmpjes e.d. met wie wel of niet gedeeld kunnen worden (1.7).		Privacy Sociale Media
	V1.5 Kan werken met sterke wachtwoorden (2.2)	Wachtwoorden	
Basisniveau 2: onderbouw voortgezet onderwijs	V2.1 Kan toegang tot gegevens en bestanden begrijpen en instellen (2.2).	Back-up	
	V2.2 Kan de rechten van programma's en apps begrijpen en instellen.	Apps	Privacy Mobiel
	V2.3 Kan het eigen profiel op een sociaal netwerk begrijpen en instellen.		Sociale Media, Privacy
	V2.4 Kan een reservekopie c.q. back-up van de eigen gegevens en bestanden maken en deze weer terughalen.	Back-up	
	V2.5 Ik weet hoe ik een update moet uitvoeren en/of hoe ik ervoor zorg dat dit standaard gebeurt	Updates	
	V2.6 Kan op een veilige manier internetbankieren gebruiken:		Internetbankieren
	V2.7 Kan nepwebsites herkennen bij online aankopen - Ziet het er te mooi uit om waar te zijn? Dan is dat het vaak ook - Koop liever alleen bij bekende websites		Online Winkelen

Basisbeveiliging	Frequentie Leerdoelen	Thema	Frequentie Leerdoelen
Wachtwoorden	2	Sociale Media	7
Nep mail of neptelefoontje	3	Draadloos internet	1
Updaten	3	Internetbankieren	3
Cybercrime	6	Online Winkelen	3
Apps	2	Privacy	10
Back-up	3	Incidenten	1
Virus	1		
Downloaden	3		

Tabel 6. Onderverdeling van basisbeveiliging en thema's a.d.h.v. veiliginternetten.nl

Bijlage 2. Curriculum.nu leerdoelen

Hieronder kan u de leerdoelen vinden zoals geformuleerd door curriculum.nu. In de laatste kolom is aangegeven of dit leerdoel is meegenomen in de baseline of niet.

Leerdoel		Meenemen
Niveau 1 (onderbouw lager onderwijs)		
1.1	dat er online veilige en minder veilige omgevingen bestaan (zoals er ook in de buitenwereld veilige en minder veilige plaatsen zijn)	✓
1.2	dat accounts beveiligd zijn met (al dan niet visuele) wachtwoorden en hoe ze daar verstandig mee om kunnen gaan	✓
1.3	dat het verstandig is om alleen te klikken op koppelingen waarvan ze de bron kennen en vertrouwen	✓
1.4	hoe ze moeten handelen als ze ongewenste content tegenkomen en wie ze hierbij om hulp kunnen vragen	Zie 1.8
1.5	dat iedereen eigenaar is van zijn eigen persoonlijke gegevens en dat anderen die niet zonder toestemming mogen gebruiken en niet mogen zien	✓
1.6	dat alles wat ze online doen, sporen achterlaat	✓
1.7	na te denken over de gevolgen van het delen van media-uitingen, zoals foto's en filmpjes	✓
1.8	wat ze kunnen doen als er iets misgaat	✓
Niveau 2 (bovenbouw lager onderwijs)		
2.1	hoe ze de veiligheid van hun digitale leefomgeving kunnen waarborgen, bijvoorbeeld door te reflecteren op het beheer van hun bestanden, gegevens en account(s), waarbij aandacht wordt besteed aan wie toegang heeft tot hun informatie	✗
2.2	op welke manieren accounts beveiligd kunnen zijn en hoe hun gegevens hiermee beschermd kunnen worden; daarbij wordt aandacht besteed aan de sterktes en zwaktes van methodes als wachtwoorden en mogelijkheden zoals biometrische beveiliging	✓
2.3	hoe ze kunnen handelen bij een (mogelijk) veiligheidsprobleem	Zie 1.8
2.4	op welke manier ze sporen achterlaten bij hun gebruik van digitale middelen. Hierbij worden ze zich bewust van de mogelijkheden die dit biedt, maar ook van de risico's die dit met zich meebrengt	✗
2.5	dat gebruikers' data vaak bij andere partijen bewaard worden. Daar zijn risico's aan verbonden en partijen hebben een verantwoordelijkheid voor de veiligheid van die data	✓
2.6	dat zij uiting moeten geven aan problemen die zij online ervaren, waarbij hun eigen veiligheid of die van anderen in het geding is	✗
2.7	welke waarde persoonsgegevens hebben voor henzelf en voor anderen en dat daarbij verschillende belangen kunnen spelen	✓
2.8	actief om te gaan met het eigenaarschap van hun gegevens, waarbij ze leren hoe ze moeten handelen als anderen daar niet zorgvuldig mee omgaan en bij wie ze dit kunnen melden	✗
2.9	dat hun aanwezigheid in (digitale) media sporen achterlaat. Hierdoor worden ze zich bewust van de manieren waarop ze gevolgd worden, welke mogelijkheden er zijn om zich hiertegen te beveiligen	✓
2.10	na te denken over de blijvende gevolgen van het plaatsen van media-uitingen, voordat ze dit daadwerkelijk doen. Daarbij is aandacht voor de persoonlijke veiligheid van henzelf en van anderen	✓
2.11	zorgvuldig te zijn met andermans gegevens en niets te plaatsen zonder toestemming en dat het strafbaar is om zonder toestemming persoonlijke gegevens van derden te delen	✓
Niveau 3 (onderbouw voortgezet onderwijs)		
3.1	welke belangen personen en partijen kunnen hebben om in het bezit te komen van de data van anderen of om zeggenschap te krijgen over digitale middelen die van anderen zijn	✗
3.2	hoe ze kunnen herkennen of hun online omgeving veilig is (denk aan toegangsrechten van applicaties, beveiligde verbindingen en gecertificeerde websites) en hoe ze die veiligheid zelf kunnen versterken door middel van tools als virusscanners, spamfilters en adblockers	✗
3.3	welke technieken er bestaan om persoonlijke gegevens te beveiligen, zoals uitgebreide beveiligingsmethodes als biometrische technieken, encryptie en tweestapsverificatie	✗

3.4	een kritische houding aan te nemen, zodat ze zich kunnen beschermen tegen huidige en toekomstige bedreigingen en kennis hebben van technieken als botnets en DDOS-aanvallen	x
3.5	dat hun persoonlijke gegevens nooit volledig beveiligd zijn, denk bijvoorbeeld aan hacking, datalekken en misbruik van Internet of Things-toepassingen. Om misbruik en identiteitsfraude te voorkomen, leren ze wat ze in dit soort gevallen zelf kunnen doen en bij welke instanties ze terecht kunnen wanneer dit henzelf niet lukt	x
3.6	een persoonlijk kader te ontwikkelen ten aanzien van online gedrag, waarbij een respectvolle houding ten opzichte van de persoonlijke integriteit de boventoon voert. Hierbij leren ze reflecteren op onveilig eigen gedrag. Bij het signaleren van ongewenst of onveilig mediagebruik door anderen leren zij anderen op hun gedrag aan te spreken en dit zo nodig te melden om het te laten verwijderen	x
3.7	dat ook bedrijven, instellingen en overheid veiligheidsrisico's lopen en welke maatregelen daartegen genomen kunnen worden	x
3.8	dat er op het gebied van cybersecurity studie- en beroepsmogelijkheden zijn	x
3.9	de werking van technologie begrijpen, die het mogelijk maakt om hun digitale sporen in de digitale wereld te volgen en te analyseren en leren hoe verschillende partijen daarvan gebruik of misbruik maken	x
3.10	op basis van begrip van digitale technologie invloed uit te oefenen op de digitale sporen die zij achterlaten. Daarbij is zowel het eigen gedrag als het benutten van technische mogelijkheden van belang	x
3.11	de inhoud van wetgeving rondom privacyaspecten te begrijpen en hiernaar te handelen; denk hierbij aan de Algemene Verordening Gegevensbescherming (AVG)	x
3.12	vanuit persoonlijk en maatschappelijk perspectief te reflecteren op maatregelen die genomen kunnen en moeten worden om privacy in de digitale wereld te beschermen	x