

PVA – Project: Cybersecurity

Hoe kunnen wij succesvol een steentje bijdragen aan de activiteit gegeven door Eva Notté?

–

Opdrachtgever: Eva Notté, Terre des Hommes

Door: Ian Valk, Arif Ulu, Max van den Bergh en Younes Budil



§1 Informatiepagina

§1.1 Auteurs

Arif Ulu

E-mail: 118724@calandlyceum.nl

Portfolio: <http://118724.webnode.nl/>

Ian Valk

E-mail: 118726@calandlyceum.nl

Portfolio: <http://www.portfolio-ian.webnode.be/over-mij/>

Younes Budil

E-mail: 120173@calandlyceum.nl

Portfolio: <https://younesbudil0.webnode.nl/>

Max van den Bergh

E-mail: 119333@calandlyceum.nl

Portfolio: maxcalandlyceumportfolio.jouwweb.nl

Groepswebsite: <https://kp1-5v.webnode.page>

§1.2 Docenten

J. Berendsen

jberendsen@calandlyceum.nl

R.M.M. Smink

rsmink@calandlyceum.nl

§1.3 Data

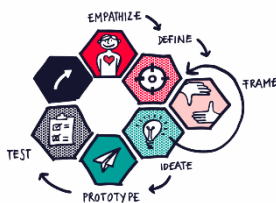
Dit project loopt van 11-09-2023 tot 13-12-2023

§2 Voorwoord

Wij hebben voor dit project de taak gekregen om een NGO te vinden. Wij hebben hier hard en druk naar gezocht. Uiteindelijk hebben wij een opdracht gekregen van de organisatie Terre des Hommes. Wij geloven er sterk in dat deze opdracht en opdrachtgever ons veel mogelijkheden zullen bieden tot zelfgroei en uitdaging. De opdrachtgever heeft al ervaring met het Calandlyceum Technasium en staat open voor een mooie en zinvolle samenwerking.

§3 Samenvatting

Online veiligheid is zeer belangrijk, al helemaal voor de jongeren die het veel gebruiken. Maar zijn zij eigenlijk wel bewust van het feit dat er erg hoge risico's zijn? Bijvoorbeeld cyberpesten, het delen van te veel persoonlijke informatie en het zogeheten 'chatting with strangers'. Veel jongeren hebben zwakke wachtwoorden, zoals hun geboortedatum of naam. Een voorbeeld hiervan kan zijn: Janvanbeek123. Deze wachtwoorden zijn absoluut niet veilig en kunnen snel door hackers ontdekt worden.



Ouders en scholen kunnen hun kinderen en leerlingen helpen met het verbeteren van online veiligheid, wat zeker een goed idee is. Aangezien wij een steeds groter aantal jongeren zien die te maken krijgen met zulke mediahackers.

Inhoudsopgave

§1 INFORMATIEPAGINA.....	1
§1.1 AUTEURS	1
§1.2 DOCENTEN	1
§1.3 DATA.....	1
§2 VOORWOORD	2
§3 SAMENVATTING	2
§4 INLEIDING	4
§5 OPDRACHTGEVER.....	5
§6 OPDRACHT	6
§7 PROBLEEMSTELLING.....	7
§8 VOORONDERZOEK.....	8
§8.1 ONLINE VEILIGHEID	8
§8.2 WAAROM IS ONLINE VEILIGHEID ZO BELANGRIJK?	8
§8.3 WAT ZIJN DE RISICO'S?	9
§8.4 MAATREGELEN.....	9
§9 ONDERZOEKSVRAAG	11
§9.1 HOOFDVRAAG	11
§9.2 DEELVRAGEN	11
§10 DELIVERABLES	12
§10.1 PLAN OPSTELLEN	12
§10.2 DEELNEMERS VERZAMELEN	12
§10.3 RICHTLIJNENFORMULIER MAKEN	12
§11 PLANNING EN TAAKVERDELING	13
§12 PROCES EN AFRONDING	14
§13 LITERATUURLIJST	15

§4 Inleiding

Onze opdrachtgever, Eva Notté van Terre Des Hommes, wil graag onze hulp gebruiken bij het VOICE project (Values, Opinions, and Insights of Children and Caregivers about E-safety). Hierbij assisteren wij haar bij het voorbereiden en uitvoeren van een bepaalde activiteit.

Als team van vier hebben wij dus een opdracht gekregen. Deze opdracht kan worden opgedeeld in twee taken; de eerste taak is het verzamelen van 8 tot 12 jongeren voor een meeting over online veiligheid. Hiervoor zullen wij ook een locatie moeten klaarmaken en toestemmingsformulieren sturen naar zowel de deelnemers als hun ouders.

De tweede taak is het ontwikkelen van richtlijnen over hoe je met jongeren kunt praten over gevoelige onderwerpen. Hierbij zullen wij niet alleen onderzoeken wat de beste manieren zijn om dit te benaderen, maar ook onze eigen feedback en visies integreren in een overzicht.

§5 Opdrachtgever

Onze opdrachtgever is Eva Notté van Terre des Hommes. Terre des Hommes is een zeer grote organisatie die ook internationaal bekend is. Terre des Hommes bestrijdt de zeer heftige en erge vormen van kinderarbeid, -handel, -prostitutie en -misbruik. Het zet zich in voor kinderrechten. De organisatie is in 1960 opgericht door Edmond Kaiser. Eva Notté is onze contactpersoon voor dit project. Zij werkt binnen Terre des Hommes als Technisch Adviseur Kindermisbruik en Onveilige Migratie.



§6 Opdracht

Zoals eerder vermeld hebben wij een opdracht die in twee taken verdeeld kan worden. Om te beginnen met de eerste; de opdrachtgever heeft ons geïnformeerd dat het de bedoeling is dat er een activiteit georganiseerd wordt voor jongeren tussen de 12-17 jaar. Dit wordt ook gedaan in 14 andere landen over de hele wereld. In deze activiteit zal het centrale onderwerp online veiligheid zijn en door middel van een aantal activiteiten, zal data en advies van jongeren verzameld worden. De eisen voor onze opdracht zijn:

- Het verzamelen van 8 tot 12 jongeren (12-17 jaar).
- Het prikken van een datum waarbij dit groepje aanwezig kan zijn voor ongeveer 2 uur voor 13 november 2023.
- Het vinden van een locatie om deze activiteit uit te voeren (bijvoorbeeld een lokaal).
- Het verspreiden van toestemmingsformulieren naar zowel jongeren als hun ouders.

Het tweede deel van de opdracht is om richtlijnen te ontwikkelen over hoe je met kinderen en jongeren kunt praten over gevoelige onderwerpen, zoals online misbruik of online veiligheid. Wij zullen onderzoeken wat de beste manieren zijn om met jongeren in gesprek te gaan over heftige zaken. Daarnaast zullen wij ook onze eigen inbreng en feedback verwerken in een verslag. Dit verslag zal vervolgens dienen als een feedbackformulier voor Terre des Hommes, om degene die zich op jongerenparticipatie richten een beter idee te geven over hoe je gevoelige onderwerpen kunt bespreken met jongeren.

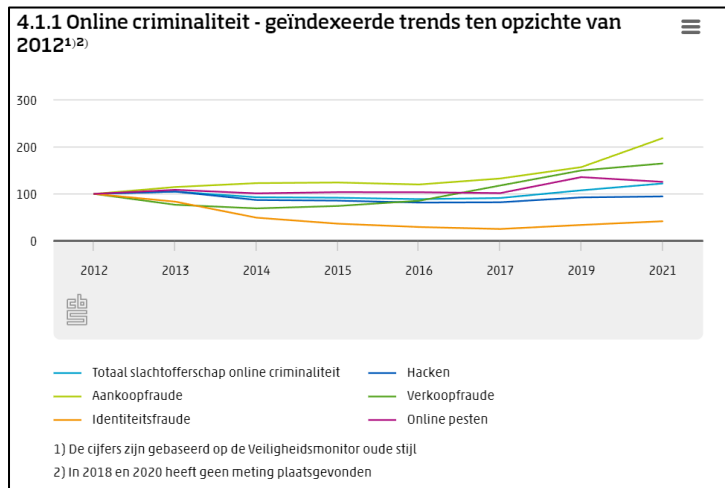
§7 Probleemstelling

Tegenwoordig is het heel normaal dat jongeren sociale media gebruiken. Het heeft veel voordelen voor iedereen, maar sociale media hebben naast deze voordelen ook veel nadelen. Een van die nadelen is cyber-pesting. Jongeren zijn vaak de dupe hiervan en dat loopt niet altijd goed af. Jongeren kunnen bijvoorbeeld depressief worden of zichzelf van sociale media scheiden.

§8 Vooronderzoek

§8.1 Online veiligheid

Veilig internetten, veel mensen denken dat het niet belangrijk is, maar niks is minder waar. Het aantal slachtoffers van cybercrime is bijna verdubbeld sinds 2013 (Centraal Bureau voor de Statistiek, 2022).



Een vorm van cybercrime waar u vast al eens van gehoord heeft is hacking. Dit wordt vaak veroorzaakt door het feit dat mensen slechte wachtwoorden gebruiken zoals bijvoorbeeld: HenkvanStegen12. De technologie van hackers wordt steeds geavanceerder. Ze gebruiken nu programma's waarmee ze makkelijk zwakke wachtwoorden kunnen kraken waardoor ze toegang kunnen krijgen tot jouw hele systeem (Centraal Bureau voor de Statistiek, 2022). Dit is maar één van de vele manieren hoe hackers te werk gaan.

Ook hebben mensen niet door hoe belangrijk hun wachtwoord eigenlijk is. Het delen van wachtwoorden met anderen, zoals vrienden of collega's, is inmiddels veelvoorkomend. Natuurlijk kan dit in veel gevallen geen kwaad, maar het meest veilige zou zijn om jouw wachtwoord voor jezelf te houden. Ook slaan veel mensen hun wachtwoord op, op een onveilige plek. Denk dan aan jouw telefoon, een briefje, of Notepad. Een grote fout die mensen maken wanneer het aankomt tot online veiligheid is het hebben van hetzelfde wachtwoord op alle apps en programma's. Wanneer een hacker toegang heeft tot je wachtwoord kan hij/zij bij al jouw programma's komen. Denk dan ook aan je bank/financiën.

Online veiligheid is iets dat tegenwoordig heel veel waarde heeft en mensen beseffen dit niet. Ook gebruiken steeds meer mensen sociale media, hierdoor hebben hackers altijd genoeg slachtoffers in het oog om te hacken.

§8.2 Waarom is online veiligheid zo belangrijk?

Velen onderschatten de consequenties van het onvoorzichtig zijn met persoonlijke gegevens, door bijvoorbeeld zwakke wachtwoorden te hebben, of door deze op een onveilige manier op te slaan. Tegenwoordig hebben hackers talloze manieren om de gegevens van een slachtoffer te verkrijgen. Als de gegevens van een gebruiker worden gestolen, kan dit drastische gevolgen hebben.

§8.3 Wat zijn de risico's?

Zoals eerder vermeld, hebben hackers vele manieren om jouw gegevens te verwerven. Om te beginnen met het feit dat ze over allerlei software beschikken. Deze software zijn ook wel als malware bekend. Hier worden er een paar beschreven:

Spyware is de term voor programma's die speciaal zijn gemaakt om de activiteit van een slachtoffer te bespioneren. Hierbij kan de hacker onder andere jouw activiteiten op het internet bekijken, toetsaanslagen zien en zelfs bespioneren via apparatuur (een voorbeeld hiervan is een webcam). Het doel hierbij is meestal om geld te verdienen, of om gegevens te stelen zonder ontdekt te worden.

Ransomware is een malware die hackers en oplichters kunnen gebruiken om de computer van een slachtoffer te ontgrendelen. Vervolgens kan een oplichter de eigenaar informeren dat hij geld moet betalen als hij weer controle wil over het apparaat.

Een **trojan** is een malware vermomd als een normaal programma of bestand, wanneer deze wordt geïnstalleerd door een gebruiker komen er allerlei gevaarlijke malware op het apparaat.

Een **virus** is een gevaarlijke software meestal met het doel om het apparaat van een gebruiker te beschadigen, door bijvoorbeeld bestanden te verwijderen en/of de computer te bestormen met schadelijke bestanden. Als gevolg wordt het getroffen apparaat erg traag, daarnaast kost het ontzettend veel tijd om weg te halen. In sommige gevallen kunnen virussen zelfs criminelen toegang geven tot je persoonlijke gegevens.

Tekens die kunnen aantonen dat je apparaat is getroffen door malware kunnen onder andere zijn:

1. Jouw computer loopt vast en/of crasht vaak.
2. Er zijn bestanden die je niet herkent.
3. Hoger CPU-gebruik dan normaal.
4. Minder goede prestaties dan gewoonlijk.
5. Over het algemeen vreemd gedrag dat door jouw apparaat wordt vertoond.

§8.4 Maatregelen

Het gebrek aan online veiligheid is dus veel gevaarlijker dan je denkt. Hoe kun je je dan beter beschermen tegen deze grote risico's?

1. Deel geen persoonlijke informatie, denk dan aan woonplaats, telefoonnummer of wachtwoorden. (Ministerie van Algemene Zaken, 2023)
2. Bedenk een sterk wachtwoord, het hebben van een sterk wachtwoord is zeer belangrijk, aangezien hackers steeds beter en geavanceerder worden in het raden van zwakke wachtwoorden d.m.v. AI/automatische systemen. Een voorbeeld van een sterk wachtwoord is: 9kO19Vjaq@@e en dus niet wachtwoorden zoals qwerty of 123456.
3. Installeer een virusscanner, deze zijn overal te vinden op het internet. Eentje die wij zouden aanraden is Malwarebytes. De beste virusscanners kosten vaak geld. Maar er zijn ook een aantal gratis virusscanners die de online veiligheid sterk vergroten. (Ministerie van Algemene Zaken, 2023)

4. Gebruik VPN's.

Er zijn nog veel meer maatregelen die je kan nemen om jouw online veiligheid te vergroten, maar met alleen deze tips kan je al een heel stuk verder komen.

§9 Onderzoeksvraag

§9.1 Hoofdvraag

De hoofdvraag geformuleerd bij dit project is:

Hoe kunnen wij succesvol een steentje bijdragen aan de activiteit die zal plaatsvinden?

§9.2 Deelvragen

- Hoe kunnen wij 8 tot 12 jongeren tussen de 12-17 jaar verzamelen en overtuigen om te participeren in de activiteit waarbij jongeren worden voorgelicht over cybercrime?
- Waar zal de activiteit waarbij jongeren worden voorgelicht over cybercrime zich plaatsvinden?
- Hoe kunnen wij het best richtlijnen op een overzichtelijke manier zetten in een feedbackformulier?

§10 Deliverables

§10.1 Plan opstellen

Voordat wij deelnemers verzamelen, is het van belang dat wij een plan opstellen om goed verder te gaan. Het is namelijk ook belangrijk dat wij nadenken over hoe wij precies deelnemers gaan zoeken en verzamelen. Ook moeten wij een toestemmingsformulier gereed hebben. Ten slotte kunnen wij bepalen waar de activiteit zich zal plaatsvinden.

§10.2 Deelnemers verzamelen

De volgende stap is om het plan uit te voeren. Wij beginnen met het verzamelen van deelnemers en wij vertellen hen alle nodige informatie. Ten slotte zullen de mensen die meedoen ook een toestemmingsformulier ontvangen.

§10.3 Richtlijnenformulier maken

Nadat de activiteit is afgelopen is de volgende taak om richtlijnen te maken en feedback te geven over hoe je gevoelige onderwerpen kunt bespreken met jongeren en kinderen. Dit zal worden gedaan in de vorm van een richtlijnenformulier. Wij zullen informatie verzamelen en onderzoek doen naar dit onderwerp. Ten slotte zullen wij ook onze eigen inbreng en visies toevoegen aan het formulier.

§11 Planning en taakverdeling

Deliverable	Verantwoordelijke	Deadline
1: Plan opstellen	Arif	1-11
2: Deelnemers verzamelen	Max	13-11
3: Richtlijnenformulier maken	Younes	29-11

Voor de volledige planning, zie bijlage 1.

§12 Proces en afronding

Max is onze contactpersoon en hij zal wekelijks contact houden met de opdrachtgever. Dit doet hij door middel van het sturen van e-mails of d.m.v. telefonisch contact. Ook zullen wij grotere gesprekken inplannen met de opdrachtgever d.m.v. een online- of fysieke meeting. Daarnaast houden wij zoveel mogelijk data bij wanneer het aankomt tot verdere progressie binnen het project.

§13 Literatuurlijst

Nidirect. (2023). Staying safe online. nidirect. <https://www.nidirect.gov.uk/articles/staying-safeonline#:~:text=Most%20people%20store%20a%20lot,of%20ways%20over%20the%20internet.>

Centraal Bureau voor de Statistiek. (2022). 4. Cybercrime. Centraal Bureau voor de Statistiek. <https://www.cbs.nl/nl-nl/longread/rapportages/2022/cybersecuritymonitor-2021/4-cybercrime>

Regan, J. (2023). Wat is spyware? Wat is spyware? <https://www.avg.com/nl/signal/what-is-spyware>

Ministerie van Algemene Zaken. (2023, 3 oktober). Welke maatregelen kan ik nemen om veilig te internetten? <https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/vraag-en-antwoord/welke-maatregelen-kan-ik-nemen-om-veilig-te-internetten>

National Cybersecurity Alliance. (2023). How to tell if your computer has a virus and what to do about it. National Cybersecurity Alliance. <https://staysafeonline.org/online-safety-privacy-basics/how-to-tell-if-your-computer-has-a-virus-what-to-do-about-it/%20https://staysafeonline.org/online-safety-privacy-basics/how-to-tell-if-your-computer-has-a-virus-what-to-do-about-it/>

§14 Bijlagen

§14.1 Bijlage 1: Planning

[Planning.xlsx](#)