Plan van Aanpak

terre des hommes

stopt kinderuitbuiting

September 2023 – Januari 2024

Cedric van Dam, Nikki van Wees, Ewout Schmitz en Ruben van der Kuij

Informatie

Auteurs

Cedric van Dam (17 jaar), klas 5v1 – Waarnemend leider

Nikki van Wees (16 jaar), klas 5v1

Ewout Schmitz (16 jaar), klas 5v1 - Contactpersoon

Ruben van der Kuij (15 jaar), klas 5v1 – Teamleider

Docenten

R. Smink, Docent O&O

rsmink@calandlyceum.nl

J. Berendsen, Docent O&O

jberendsen@calandlyceum.nl

De opdrachtgever

Terre des Hommes, vertegenwoordigd door Eva Notté, houdt zich bezig met het bestrijden van kinderuitbuiting.

Data

Dit project loopt van 20 september 2023 tot circa 10 januari 2024

Contact

Cedric van Dam: Mailadres – 118522@calandlyceum.nl, Portfolio – https://portfolioced.webnode.nl/

Nikki van Wees: Mailadres – 119379@calandlyceum.nl, Portfolio – https://portfolio6817.webnode.nl/

Ewout Schmitz: Mailadres – 119357@calandlyceum.nl, Portfolio – http://ewoutschmitz.com/

Ruben van der Kuij: Mailadres – 119275@calandlyceum.nl, Portfolio – https://rubeniscool123-nl.jouwweb.nl/

Voorwoord

Technologie wordt steeds geavanceerder en het wordt steeds normaler om meerdere apparaten te bezitten met toegang tot het internet. Tegenwoordig krijgen kinderen al op een steeds jongere leeftijd een telefoon maar vaak weten ze niet welke gevaren er in het internet schuilen. Ook ouders hebben hier moeite mee. Ze kunnen niet goed controleren wat de kinderen doen op het internet en zelf weten ze vaak ook niet welke gevaren er allemaal zijn. Daarom is het belangrijk om ouders te informeren over wat de gevaren zijn van het internet en hoe ze hun kinderen kunnen helpen om zich te beschermen tegen deze gevaren.

Samenvatting

Online veiligheid is een belangrijk iets dezer dagen dankzij verschillende soorten internetcriminaliteit. Mensen kunnen slachtoffer worden van phishing, aankoop- en verkoopfraude, hacking en meer. Hoewel er veel oplossingen zijn voor internetcriminaliteit, zowel kinderen als volwassenen weten er vaak niet genoeg van en kunnen daardoor slachtoffer worden van internetcriminaliteit. Wij gaan een onderzoek doen naar verschillende soorten internetcriminaliteit en hoe je het kunt vermijden, en ook gaan we een campagne ontwikkelen voor ouders over hoe ze hun kinderen kunnen helpen en adviseren als het gaat om internetcriminaliteit.

Inhoudsopgave

Inleiding

§1.1 onderwerp

Sinds de introductie van het internet zijn er mensen geweest die gebruik hebben gemaakt van het feit dat ze zich achter hun scherm kunnen verschuilen. Mensen zijn nieuwe soorten aan vallen gaan ontwikkelen waardoor ze dingen als persoonlijke informatie of geld kunnen stelen van nietsvermoedende gebruikers van het internet.

Tegenwoordig worden apparaten steeds kleiner gemaakt en dit geeft de optie om ze ook mee te kunnen nemen. Aangezien veel bezorgde ouders het fijn vinden om een veilige situatie te bieden voor hun kinderen, ook al zijn ze buiten of op school, geven ouders hun kinderen op een steeds jongere leeftijd een telefoon.

Dit zorgt ervoor dat het kind de ouders bijvoorbeeld kan bellen, of dat de ouders kunnen zijn waar het kind zich op dat moment bevindt, maar het creëert ook een aparte, indirecte en onveilige situatie.

Kinderen zelf weten natuurlijk niet veel over online criminaliteit, laat staan over hoe ze zichzelf ertegen kunnen beschermen. Dit wordt ze nauwelijks meegegeven, en dit zorgt ervoor dat criminelen steeds meer hun gang kunnen gaan.

Maar kinderen zijn niet de enigen die kwetsbaar zijn. Ook ouders weten vaak niet hoe ze zichzelf veilig kunnen houden en hoe ze hun kinderen advies kunnen geven over hoe ze zich online kunnen beschermen. Maar hoe los je dit op? En hoe help je ouders over hoe ze de juiste adviezen kunnen geven aan hun kinderen?

§1.2 Opdrachtgever

Terre des Hommes is een NGO die zich focust op het bestrijden van kinderarbeid, seksuele uitbuiting van kinderen, noodhulp voor kinderen en meer rondom de uitbuiting van kinderen. Terre des Hommes haalt kinderen uit uitbuitingssituaties en zorgt ervoor dat kinderen zich in een veilige omgeving kunnen ontwikkelen. Ook geven ze basisbehoeften als eten en water aan kinderen in noodsituaties, om mogelijke uitbuiting te voorkomen.

§1.3 Opdracht

De opdracht is om een campagne te ontwikkelen die ouders helpt met het geven van adviezen over internetcriminaliteit aan hun kinderen. Dit helpt kinderen indirect en gaat de online uitbuiting van kinderen tegen.

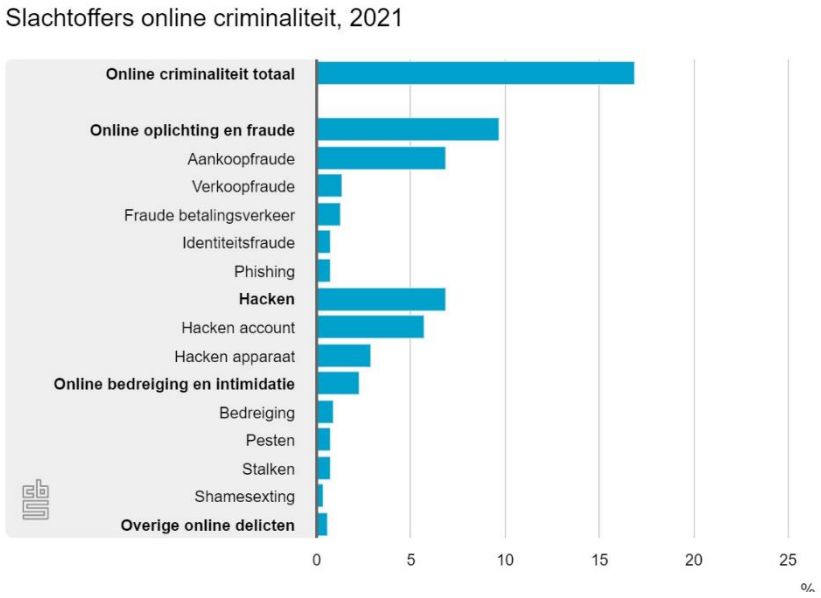
§1.4 Probleemstelling

Telefoons, laptops, Televisie, elektronica is steeds, met ieder voorbijgaand jaar, belangrijker in de wereld. Dit is natuurlijk prachtig maar heeft natuurlijk ook zijn gevaren. Meer en meer kinderen hebben op steeds jongere leeftijd hun eigen mobiele apparaten.
Hoe beschermen we dan de kinderen?
Kinderen lopen dan veel gevaar. Opgelicht worden, cyberpesten, bedreigingen en ongewenste afbeeldingen zijn niet dingen waar kinderen aan blootgesteld moeten worden.

Met de ook groeiende schermtijd gemeten door Nederland en de EU is er meer en meer kans voor cybercriminelen om hun slag te slaan. Dit is een groot probleem.

Vooronderzoek (verdieping)

Volgens een onderzoek verricht door de Nederlandse Omroep Stichting (NOS), zit de gemiddelde scholier maar liefst vijf uur per dag op zijn of haar telefoon. Veel jongeren in Nederland zijn redelijk goed op de hoogte van onveiligheden op het internet, maar dat neemt niet weg van het feit dat 17 procent van de Nederlandse bevolking in 2021 volgens een onderzoek van het Centraal Bureau van de Statistiek (CBS) slachtoffer is geweest van internetcriminaliteit.



§2.1 Verschillende soorten internetcriminaliteit

Zoals in de afbeelding hierboven te zien is zijn er veel verschillende vormen van internetcriminaliteit. De meest voorkomende vormen zijn in de afbeelding afgebeeld maar er zijn nog veel meer vormen van internetcriminaliteit, alleen komen deze significant minder vaak voor.

§2.2 Aankoopfraude

Ongeveer 1,2 miljoen Nederlanders zijn in 2021 volgens het Centraal Bureau van de Statistiek slachtoffer geworden van aankoopfraude. Dit betekent dat een klant betaalt voor een product, maar dat product vervolgens niet geleverd krijgt. Zo verliest de klant geld terwijl de leverancier van het product verdwijnt zonder veel mogelijkheden om vervolgd te worden. Aankoopfraude kan fysiek plaatsvinden maar in bijna alle gevallen gebeurt het online. Er zijn veel manieren om aankoopfraude te voorkomen. Er zijn bijvoorbeeld politielijsten waarop bekeken kan worden of een webshop wel juist is. Ook is er een databank waar gecontroleerd kan worden of er meldingen zijn gedaan over de webshop. Daarnaast kan er op het taalgebruik van de verkoper gelet worden. Als de verkoper niet professioneel overkomt bij het verkopen van een duur of officieel product, dan kan dat een teken zijn dat de verkoper je wil bedriegen. Tot slot is het een handig idee om het rekeningnummer te controleren voordat er bedragen over worden gemaakt. Komt de naam waaronder het rekeningnummer staat niet overeen met de naam van de verkoper, dan kan dat een teken zijn van een mogelijke bedrieger.

§2.3 Verkoopfraude

Ongeveer 245.000 Nederlanders zijn in 2021 volgens het Centraal Bureau van de Statistiek slachtoffer geworden van verkoopfraude. Verkoopfraude is het omgekeerde van aankoopfraude. Iemand verkoopt een product maar ontvangt vervolgens geen geld van de klant. Bij verkoopfraude kan er gevraagd worden aan de bank om een terugstortverzoek te doen aan de dader. Dit houdt in dat de dader een verzoek krijgt om het schuldige geld alsnog te betalen. Doet de dader dit niet binnen drie weken, dan krijgt de leverancier de contactgegevens van de dader. Deze gegevens kunnen doorgestuurd worden naar een deurwaarder die de dader in kwestie zal lastigvallen totdat het verschuldigde bedrag betaald wordt. Betaalt de dader nog steeds niet, dan wordt er beslag gelegd op de spullen van de dader, worden de spullen verkocht, en krijgt de leverancier alsnog het geld terug op basis van de waarde van de afgenomen spullen. Ook verkoopfraude kan voorkomen worden door goed op te letten wat het gedrag van de klant is. Vooraf betalen of contant betalen zijn ook erg simpele manieren om verkoopfraude te voorkomen.

§2.4 Identiteitsfraude

Ongeveer 140.000 Nederlanders zijn in 2021 volgens het Centraal Bureau van de Statistiek slachtoffer geworden van identiteitsfraude. Dit houdt in dat een crimineel misbruik maakt van valse of gestolen gegevens. Identiteitsfraude is een erg gevaarlijke vorm van fraude. Een crimineel kan identiteitsfraude namelijk gebruiken om een andere vorm van internetcriminaliteit uit te voeren zonder dat ze zelf in gevaar komen. Ze kunnen iemands gegevens stelen en gebruiken waardoor een deurwaarder naar het adres zou kunnen gaan van een eerlijke burger, om een betaling te vragen die niet is gemaakt door een heel ander persoon op een hele andere plek. Slachtoffer worden van identiteitsfraude is moeilijk te voorkomen. Voorkom het invullen van gegevens bij websites die er verdacht uitzien. Slachtoffers van identiteitsfraude kunnen een melding maken bij het Centraal Meldpunt Identiteitsfraude (CMI), die hun bank op de hoogte kan brengen. Ook kan de politie geraadpleegd worden bij identiteitsfraude.

§2.5 Phishing

Ongeveer 140.000 Nederlanders zijn in 2021 volgens het Centraal Bureau van de Statistiek slachtoffer geworden van Phishing. Dit houdt in dat een crimineel malware op apparaten probeert te krijgen. Hiermee kunnen ze online activiteit volgen, toegang krijgen tot gegevens en wachtwoorden en ze kunnen ook te weten komen over persoonlijke zaken. Er zijn erg veel vormen van Phishing, waaronder e-mail spoofing, URL Phishing, Clone Phishing, Invoice Phishing, Phishing via gedeelde documenten, Phishing via smartphone apps, Phishing via pop-up vensters, Phishing via de zoekmachines, Phishing door filters te omzeilen en Catphishing. Bij e-mail Phishing probeert een crimineel door middel van een e-mail mensen op een specifieke kwaadwillende website te krijgen, die vaak er vrijwel exact hetzelfde uit ziet als een echte, goedwillende website. Ze proberen mensen zover te krijgen dat ze inloggegevens invullen op de kwaadwillende site, waarmee ze dan toegang krijgen tot het account voor de goedwillende website. Vishing is een vorm van Phishing waarbij de crimineel door middel van een telefoongesprek of ingesproken bericht iemand wil overtuigen om iets voor ze te doen. Of dit nou leidt tot toegang hebben tot inloggegevens voor een bank of het infiltreren van iemands laptop verschilt per geval maar de crimineel kan veel kanten op. Smishing is vaak gericht op het achterhalen van bankgegevens door middel gebruik te maken van een nepwebsite. De crimineel stuurt een link die net lijkt op de echte link van een goedwillende site, vaak met een bericht erbij dat je drukt om snel actie te ondernemen. Hierdoor hopen criminelen dat de

ontvanger in paniek raakt en hun gegevens invult bij de nepwebsite, waardoor ze toegang krijgen tot het account op de echte website.

Phishing kan voorkomen worden door goed te letten op van wie een bericht komt, en door goed te kijken of links of bestanden wel kloppen met wat het echt zou moeten zijn.

§2.6 Account hacking

Zoals eerder beschreven is account hacking een poging van een crimineel om in een account te komen. Ongeveer een miljoen Nederlanders is in 2021 slachtoffer geworden van account hacking. Er zijn twee grote gevaren bij account hacking. Het eerste gevaar is dat de crimineel informatie over mensen kan winnen die privé gehouden hoort te worden. Het tweede gevaar is dat de crimineel door middel gebruik te maken van iemands account onder hun naam dingen kan gaan doen die die persoon niet zou doen. Een voorbeeld hiervan is het sturen van carrièreslopende e-mails naar al de slachtoffers professionele contacten. Een andere mogelijkheid is het adverteren van een eigen bedrijf door middel gebruik te maken van jouw contacten. Account hacking is te voorkomen door regelmatig wachtwoorden te veranderen naar wachtwoorden die niet op het oude wachtwoord lijken, en door dezelfde wachtwoorden niet bij andere accounts te gebruiken.

§2.7 Apparaat en systeem hacking

Ongeveer 510.000 Nederlanders zijn volgens onderzoek van het Centraal Bureau van de Statistiek in 2021 slachtoffer geworden van apparaat hacking. Dit houdt in dat een apparaat door een crimineel binnengedrongen wordt. Meestal wordt malware gebruikt om een systeem binnen te dringen. Vervolgens kan de hacker kiezen tussen informatie verzamelen of het systeem zo snel mogelijk te verstoren. Malware kan bijvoorbeeld een systeem binnendringen door een verkeerd bestand te downloaden, maar ook kan malware op een USB-stick gezet worden. Zo kan iemand ook fysiek een systeem binnendringen. Dit betekent dat grote bedrijven ook op moeten letten dat ze geen mensen aannemen die alleen bij het bedrijf ''werken'' om informatie te lekken of chaos te veroorzaken binnen het bedrijf. Er zijn soms gevallen waarbij malware gebruikt wordt om een systeem te verstoren. De crimineel geeft het bedrijf dan een ultimatum. Ze moeten kiezen tussen heel veel verlies draaien vanwege geen toegang tot de systemen, of ze moeten een grote som aan geld overmaken aan de criminelen zodat de criminelen hun bedrijf verlossen van de malware. Hacken van welke vorm ook wordt in Nederland over het algemeen bestraft door een maximum van vier jaar celstraf en/of een boete van €21.750 krijgen, maar bij hele erge gevallen van hacking kan de straf veel hoger gesteld worden.

§2.8 Bedreiging

Ongeveer 160.000 Nederlanders zijn volgens het Centraal Bureau van de Statistiek in 2021 slachtoffer geworden van online bedreigingen. Van dreigbrieven tot verbale mishandeling, bedreigingen komen in alle vormen en maten. Er zijn te veel verschillende vormen van bedreiging om allemaal te behandelen in dit vooronderzoek, maar de gevolgen voor beide actoren zijn wel te voorspellen. Bedreigd worden kan het leven mentaal voor iemand erg zwaar maken. Een slachtoffer wordt afhankelijk van de bedreiging namelijk in veel gevallen erg paranoïde. Een slachtoffer kan ervoor kiezen om thuis te blijven gedurende een lange periode. Ook kan iemand er een angststoornis aan overhouden. Ben je zelf slachtoffer van bedreiging, zorg dan dat je anderen op de hoogte brengt van de bedreigingen. Je wordt ook aangeraden om aangifte te doen bij de politie. Afhankelijk van de ernst

van de bedreigingen kan de politie per situatie anders handelen. De politie kan kiezen om niks te doen, maar kan ook een vervolgonderzoek doen om achter de dader te komen in geval die nog niet bekend is. Is de dader wel bekend kiest de politie er in veel gevallen voor om de dader per situatie aan te pakken of dit nou leidt tot het aanspreken van de dader, tot een celstraf hangt bij bedreigingen dus erg af van de ernst van de situatie.

§2.9 Pesten

Ongeveer 140.000 Nederlanders zijn volgens het Centraal Bureau van de Statistiek in 2021 slachtoffer geworden van pesten. Pesten is meestal een minder zware, maar soortgelijke vorm van bedreiging. De gevolgen voor het slachtoffer zijn meestal niet paranoïde worden of een angststoornis oplopen, maar niet uit huis willen komen is wel een mogelijk gevolg van pesten. Als slachtoffer kunt u ook depressief worden als gevolg van een tekort aan vriendelijk sociaal contact. Verbaal pesten is (met uitzonderingen) niet illegaal. Fysiek pesten is vaak niet toegestaan omdat geweld (met uitzonderingen) vaak illegaal is in Nederland. Bij pesten helpt het vaak om onzekerheden te delen met een vertrouwenspersoon. Ook kan het slachtoffer de dader aangeven bij een ander persoon (afhankelijk van de werk/schoolsituatie van het slachtoffer). Is het slachtoffer nog een scholier dan kan de dader worden aangegeven bij de schoolleiding. In het bedrijfsleven kan dit gedaan worden bij een supervisor.

§2.10 Stalken

Ongeveer 140.000 Nederlanders zijn volgens het Centraal Bureau van de Statistiek in 2021 slachtoffer geworden van stalken. Dit houdt in dat een stalker een slachtoffer opzettelijk langdurig lastigvalt. Vaak komt de dader door middel van onderzoek, achter informatie van het slachtoffer. Het slachtoffer kan lastiggevallen worden op vele verschillende manieren. Hieronder vallen bedreigingen, constante telefoontjes, achtervolgingen en dingen bestellen op naam van het slachtoffer. In principe heeft iedere stalker een motief. Dit kan bijvoorbeeld zijn dat een stalker een obsessie heeft met het slachtoffer. Stalken is strafbaar als het slachtoffer genoeg bewijs heeft. Het is dus handig als slachtoffer om te zorgen dat u niet alleen over straat loopt en dat meerdere mensen op de hoogte zijn van uw informatie. Vervolgens kan het slachtoffer zo veel mogelijk bewijs verzamelen voor het geval u een rechtszaak wilt spannen tegen de dader. Dit bewijs is ook handig om te hebben als het slachtoffer serieus genomen wil worden bij de politie als het slachtoffer kiest om aangifte te doen.

§2.11 Shamesexting

Ongeveer 70.000 Nederlanders zijn volgens het Centraal Bureau van de Statistiek in 2021 slachtoffer geworden van shamesexting. Dit houdt in dat expliciet beeldmateriaal van het slachtoffer ongevraagd wordt verspreid. Dit heeft enorme gevolgen voor het slachtoffer. Het kan erg beschamend zijn voor het slachtoffer en in veel gevallen worden de slachtoffers buitengesloten en uitgelachen. Dit kan leiden tot depressie en soms zelfs tot zelfmoord. Shamesexting moet dus erg serieus genomen worden. Als slachtoffer kunt u aangifte doen als u concreet bewijs heeft van dat specifieke mensen het expliciete materiaal opgeslagen of doorgestuurd hebben zonder toestemming van het slachtoffer. De straf die wordt gegeven aan de dader(s) ligt bij de politie of in het geval van een rechtszaak de rechter(s).

Onderzoeksvraag

§3.1 Onderzoeksvraag

Wat moeten ouders weten over veiligheid online om hun kinderen te kunnen ondersteunen?

§3.2 Deelvragen

1. Wat zijn de gevaren online?
2. Welke gevaren online moeten ouders kennen?
3. Van welke gevaren moeten ouders hun kinderen van tevoren waarschuwen?
4. Hoe kunnen ouders hun kinderen ondersteunen met deze online gevaren?

§3.3 Hypothese

Ouders moeten weten welke soorten internetcriminaliteit er bestaan en hoe ze het kunnen vermijden.

Deliverables

§4.1 Zoeken participanten voor focusgroep

Voor de focusgroep die gevraagd wordt over online veiligheid zoeken we samen met de teams van Max en Sanae twee groepen van acht tot twaalf kinderen tussen de leeftijden van twaalf en zeventien jaar. Hierbij zoeken we ook een datum vóór 13 november waarop die kinderen aanwezig kunnen zijn voor twee tot twee en een half uur. We zoeken hier ook een plek voor uit en we vragen om toestemming van de jongeren en hun ouders.

Opleverdatum: Uiterlijk 13-11-2023

§4.2 Vooronderzoek online veiligheid

Ouders weten zelf vaak niet welke gevaren er tegenwoordig op het internet zijn. Daarom doen we eerst een kort onderzoek naar de verschillende gevaren op het internet en hoe je ze kunt vermijden. Dit onderzoek bouwt voort op het vooronderzoek dat we al gedaan hebben.

Opleverdatum: Uiterlijk 16-10-2023

§4.3 Concreet product

Op basis van het vooronderzoek leveren we een campagne op in de vorm van een flyer, two-pager, website, workshop of nog nader te bedenken activiteit op. In de campagne moet aan ouders duidelijk worden welke gevaren er zijn op het internet en hoe ze hu kinderen advies kunnen geven over hoe ze zichzelf veilig houden op het internet.

Opleverdatum: Uiterlijk 8-1-2024

Planning

Wie is verantwoordelijk?	Waar is deze persoon verantwoordelijk voor?	Wanneer is deze taak af?	Waaraan moet het geleverde werk voldoen?
Ruben	*Planning en taakverdeling*	4-okt	De planning is voltooid met onderstaande eisen.
Ruben	Wie is verantwoordelijk?	4-okt	In de planning staat duidelijk wie verantwoordelijk is voor een taak.
Ruben	Waar is dit persoon verantwoordelijk voor?	4-10-2023	In de planning staat duidelijk wat de taak is.
Ruben	Wanneer is deze taak af?	4-10-2023	In de planning staat duidelijk wanneer deze taak af is.
Ruben	Waaraan moet het geleverde werk voldoen?	4-10-2023	In de planning staat duidelijk wat de eisen zijn van een taak.
Ruben	*Plan van Aanpak*	13-okt	Het plan van aanpak met onderstaande eisen is voltooid.
Ruben	Voorpagina	9-okt	Een aantrekkelijke voorkant, met titel project, bedrijf van opdrachtgever, school, namen auteurs (leerlingen). Houd info beknopt. Uitgebreide info komt op de informatiepagina.
Ruben	Informatiepagina	9-10-2023	Hier komt meer info over de auteurs en info over de opdrachtgever, experts, docenten, de start- en einddatum van het project, klassen, links naar persoonlijke portfolio's, etc. Etc.
Ewout	Voorwoord (aanleiding)	11-10-2023	Schrijf in de inleiding de informele informatie zoals waarom we het project graag doen, hoe we de opdrachtgever hebben gevonden, wie wij zijn (eventueel) en wie we willen bedanken voor bijdrage aan het project.
Nikki	Omschrijving opdrachtgever	11-okt	Vertel iets over de geschiedenis/achtergrond van het bedrijf/de organisatie van de opdrachtgever. Vertel ook iets over de professionele achtergrond van de opdrachtgever zelf.
Ruben	Probleemstelling	13-okt	Formuleer op een correcte manier een antwoord op de vraag van welk probleem we op gaan lossen.
Nikki	Omschrijving opdracht	11-okt	Omschrijf duidelijk de opdracht, de relevantie voor het bedrijf en het gewenste eindresultaat.

Cedric	Vooronderzoek	13-okt	Doe een klein onderzoek over het onderwerp van de opdracht. Noteer de bronnen in de literatuurlijst door middel gebruik te maken van APA stijl.
Ruben	Theoretisch kader	13-okt	Als er ingewikkelde woorden of processen zijn in het document noteer je die en leg je die uitgebreid met veel diepgang uit in het theoretisch kader.
Ewout	Deliverables	13-okt	Er wordt voor alles wat we opleveren duidelijk beschreven welke deelopdracht op welk moment af is. Maak hierdoor alles overzichtelijker voor de opdrachtgever.
Cedric	Onderzoeksvraag	13-okt	Het programma van eisen is voltooid en het voldoet aan de bijbehorende eisen.
Ruben	Planning (voor de opdrachtgever)	13-okt	Geef een simpele versie van de planning waar instaat welke deliverable we op welk moment inleveren.
Nikki	Proces en afronding	11-okt	Beschrijf duidelijk aan de opdrachtgever hoe het proces verloopt en wie contact houdt. Wanneer zijn de go/no go momenten en hoe vinden ze plaats? Op welke manier overleggen docenten en opdrachtgevers? Wanneer is de eindpresentatie en hoe vindt de beoordeling plaats?
Ewout	Literatuurlijst	13-okt	Geef de gebruikte bronnen weer in de literatuurlijst door middel gebruik van APA stijl.
Ewout	Bijlagen	13-okt	Zet alle bijlagen aanklikbaar en werkend overzichtelijk onder elkaar. Zorg dat het duidelijk is wat je gaat zien als je ergens op drukt.
Ewout	Lay-out	13-okt	Maak een aantrekkelijke, strakke lay-out die het lezen van ons PvA leuker maakt. Alle lettertypes zijn gelijk, afbeeldingen zijn genummerd en er wordt naar deze afbeeldingen (en/of tabellen/grafieken) verwezen in de tekst.

Cedric	*Groepswebsite*	n.v.t.	De groepswebsite is af met de onderstaande eisen voltooid.
Cedric	Startpagina	n.v.t.	Er is een startpagina met informatie over het Calandlyceum en het vak O&O.
Cedric	Over ons	n.v.t.	Er is een pagina met wat tekst over ons en onze portfolio's en POP's.
Cedric	Contactpagina	n.v.t.	Er is een contactpagina met onze namen en e-mails.
Cedric	Project	n.v.t.	Op de procespagina staan al onze deliverables met een mooie lay-out weergegeven. Alle deliverables zijn apart aanklikbaar.

Nikki	*Eindproduct*	8-1-2024	Eindproduct is voltooid en er is voldaan aan de onderstaande eisen.
Ruben	Ideeën	1-11-2023	Er moet gebrainstormed worden over mogelijke ideeën. Deze ideeën worden lichtelijk uitgewerkt getoond aan de opdrachtgever die een go/no go geeft.

Cedric	Concepten + conceptkeuze	6-11-2023	Presenteer visueel de concepten en leg uit welk concept is gekozen om uit te werken en waarom dat het gekozen concept is. Leg ook uit waarom de andere concepten niet gekozen zijn.
Ruben	Uitwerking en materialisatie	20-12-2023	Werk het gekozen idee uit. Let op: materiaalkeuze, detaillering (technische tekeningen), productiemethode, kostprijsberekeningen, businessplan (hoe wordt hier geld door verdiend?).
Ewout	Iteraties en optimalisatie	1-1-2024	Laat hier alle verschillende ontwerpen zien. Welke veranderingen zijn gemaakt om het eindontwerp te verbeteren?
Nikki	Evaluatie eindproduct	8-1-2023	Test het eindproduct bij de doelgroep. Voldoet het product aan het programma van eisen?

Nikki	*Eindrapport*	10-1-2024	Het eindrapport met de volgende pagina's/eisen is voltooid.
Cedric	Voorpagina	25-12-2023	Een aantrekkelijke voorkant, met titel project, bedrijf van opdrachtgever, school, namen auteurs (leerlingen). Houd info beknopt. Uitgebreide info komt op de informatiepagina.
Ruben	Informatiepagina	25-12-2023	Hier komt meer info over de auteurs en info over de opdrachtgever, experts, docenten, de start- en einddatum van het project, klassen, links naar persoonlijke portfolio's, etc. Etc.
Ewout	Voorwoord (aanleiding)	25-12-2023	Schrijf in de inleiding de informele informatie zoals waarom we het project graag doen, hoe we de opdrachtgever hebben gevonden, wie wij zijn (eventueel) en wie we willen bedanken voor bijdrage aan het project.
Ewout	Samenvatting	3-1-2024	Op een aparte pagina vat je je project samen: o.a. aanleiding, aanpak van het project en het resultaat.
Cedric	Inhoudsopgave	10-1-2024	De pagina's zijn genummerd en er staat op welke pagina een kopje begint.
Cedric	Inleiding	25-12-2023	Inhoudelijke inleiding op het onderwerp van je project. Hier kun je randinformatie geven over de casus. Dit stuk moet inhoudelijk interessant zijn voor de professional en interesse van de lezer wekken voor het onderwerp.
Ruben	Omschrijving opdrachtgever	25-12-2023	Vertel iets over de geschiedenis/achtergrond van het bedrijf/de organisatie van de opdrachtgever. Vertel ook iets over de professionele achtergrond van de opdrachtgever zelf.
Ruben	Probleemstelling	25-12-2023	Formuleer op een correcte manier een antwoord op de vraag van welk probleem we op gaan lossen.
Ruben	Omschrijving opdracht	25-12-2023	Omschrijf duidelijk de opdracht, de relevantie voor het bedrijf en het gewenste eindresultaat.
Cedric	Vooronderzoek	25-12-2023	Doe een klein onderzoek over het onderwerp van de opdracht. Noteer de bronnen in de literatuurlijst door middel gebruik te maken van APA stijl.
Cedric	*Plan van Aanpak*	13-10-2023	Het plan van aanpak met alle eisen die er onder vallen is voltooid en staat in het rapport.

Ruben	*Programma van Eisen*	13-10-2023	Het programma van eisen is af met alle eiden die er onder vallen voltooid en staat in het rapport.
Ewout	Deliverables	13-10-2023	De deliverables die we hebben afgesproken staan in het eindrapport. Indien nodig staat het in de bijlagen.
Ruben	*Planning en taakverdeling*	4-10-2023	De planning met alle eisen die er onder vallen is voltooid en staat in het rapport.
Ewout	Proces en afronding (hoort bij samenvatting)	25-12-2023	Beschrijf duidelijk hoe het proces verlopen is en hoe we contact hebben gehouden.
Nikki	*Eindproduct*	8-1-2024	Eindproduct is voltooid en er is voldaan aan de bijbehorende eisen.
Ewout	Conclusie	10-1-2023	Concludeer of het ontwerp een succes zou kunnen zijn.
Ruben	Aanbeveling	10-1-2023	Geef aanbevelingen over hoe ons ontwerp beter onderzocht of uitgewerkt zou kunnen worden om het nog beter te maken.
Ruben	Nawoord	10-1-2023	Beschrijf hoe (leuk) het was om dit project uit te voeren. (Blijf bij voorkeur zo positief mogelijk).
Cedric	Literatuurlijst	10-1-2023	Geef de gebruikte bronnen weer in de literatuurlijst door middel gebruik van APA stijl.
Ruben	Bijlagen	10-1-2023	Zet alle bijlagen aanklikbaar en werkend overzichtelijk onder elkaar. Zorg dat het duidelijk is wat je gaat zien als je ergens op drukt.
Cedric	Lay-out	10-1-2023	Maak een aantrekkelijke, strakke lay-out die het lezen van ons rapport leuker maakt. Alle lettertypes zijn gelijk, afbeeldingen zijn genummerd en er wordt naar deze afbeeldingen (en/of tabellen/grafieken) verwezen in de tekst.

Proces en Afronding

Wij overleggen met de opdrachtgever via de mail minimaal één keer elke week, zodat de opdrachtgever op de hoogte blijft dat we bezig zijn en waar we mee bezig zijn. Ewout is de persoon die contact houdt met de opdrachtgever. De eindpresentatie is op 10 januari. De beoordeling wordt gedaan op basis van de beoordeling van de opdrachtgever over ons eindproduct en de lerares' beoordeling.

Bronnen

APA PsycNet. (z.d.). https://psycnet.apa.org/record/2004-10365-008

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: Enhancing e-safety awareness among young people. *Computer Fraud & Security*, *2009*(7), 13–19. https://doi.org/10.1016/s1361-3723(09)70088-0

Binns, R. (2023). Screen Time Statistics 2023. *Independent Advisor*. https://www.independent.co.uk/advisor/vpn/screen-time-statistics#:~:text=Overall%2C%20the%20average%20global%20screen,2022's%20average%20of%203hrs%2014mins

Centraal Bureau voor de Statistiek. (2022, 28 februari). 2,5 miljoen Nederlanders in 2021 slachtoffer van online criminaliteit. *Centraal Bureau voor de Statistiek*. https://www.cbs.nl/nl-nl/nieuws/2022/09/2-5-miljoen-nederlanders-in-2021-slachtoffer-van-online-criminaliteit

DNS Belgium. (z.d.). *12 soorten phishing*. https://www.dnsbelgium.be/nl/slim-online/12-soorten-phishing

Dombrowski, S. C., Gischlar, K. L., & Durst, T. (2007). Safeguarding young people from cyber pornography and cyber sexual predation: a major dilemma of the internet. *Child Abuse Review*, *16*(3), 153–170. https://doi.org/10.1002/car.939

Hoe voorkom je internetoplichting? - Fidus. (z.d.). Fidus.nl. https://fidus.nl/nieuws/hoe-voorkom-je-internetoplichting

Moody, R., & Moody, R. (2022). Statistieken van schermtijd: gemiddelde schermtijd in de VS vergeleken met de rest van de wereld. *Comparitech*. https://www.comparitech.com/nl/statistieken-van-schermtijd/

(Online) Beledigen en bedreigen. (z.d.). vraaghetdepolitie.nl. https://www.vraaghetdepolitie.nl/pesten-en-online/online-beledigen-en-bedreigen

"Telefoongebruik in 2 jaar tijd met 30 procent gestegen". (2022, 12 januari). RTL Nieuws. https://www.rtlnieuws.nl/tech/artikel/5280567/telefoon-gebruik-smartphone-gemiddeld-uur-dag

The State of Mobile in 2022: How to Succeed in a Mobile-First World as consumers spend 3.8 trillion hours on mobile devices | Data.ai blog. (z.d.). data.ai. https://www.data.ai/en/insights/market-data/state-of-mobile-2022/

Wat is aan- en verkoopfraude? (z.d.). politie.nl. https://www.politie.nl/informatie/wat-is-aan--en-verkoopfraude.html