TEKNOLOGIFORSTÅELSE

7. KLASSE DANSK

Dage med Data - digitale fodspor og datasikkerhed.

Teknologiforståelse i folkeskolen

KØBENHAVNS PROFESSIONS HØJSKOLE | LÆRE MIDDEL DK | VIA University College | UCN | RAMBØLL

INDHOLDSFORTEGNELSE

1. Forløbsbeskrivelse 3
1.1 Beskrivelse 3
1.2 Rammer og praktiske forhold 4

2. Mål og faglige begreber 5

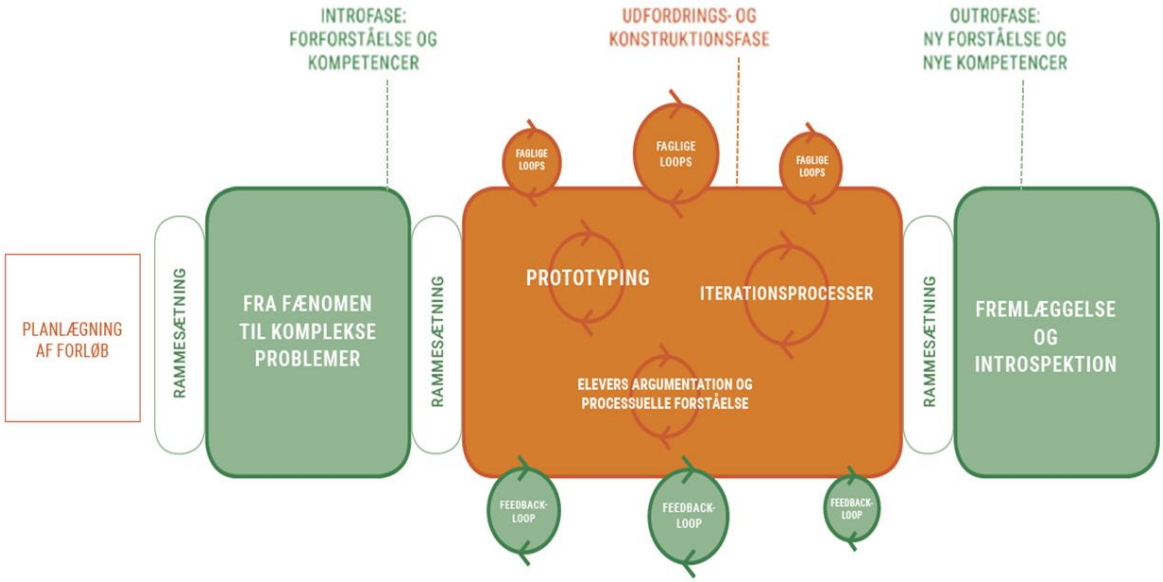
3. Forløbsnær del 8
3.1 Introfase: Forforståelse og kompetencer 8
3.2 Udfordrings- og konstruktionsfase 13
3.3 Outrofase: Ny forståelse og nye kompetencer 15

4. Perspektivering 16
4.1 Evaluering 16
4.2 Progression 16
4.3 Differentieringsmuligheder 16
4.4 Særlige opmærksomhedspunkter 16

1. Forløbsbeskrivelse

Forløbet er bygget op over det didaktiske format for prototyperne med en introducerende del, en mere undersøgende/eksperimenterende del og en outro-del med opsamlinger og evalueringer, se figur 1.
Der arbejdes i designprocessens introfase med aktivering af elevernes forforståelse for datasikkerhed og digitalt selvforsvar. Forforståelsen forsøges også aktiveret i forhold til begrebet data og hvordan vores digitale fodspor gennemsyrer alt vores færden i de fysiske og digitale miljøer. Gennem stilladserede undersøgelses- og designprocesser etableres den nødvendige baggrundsviden om hvad man skal være opmærksom på omkring egen og andres digitale sikkerhedsadfærd. Eleverne indsamler, udvælger og omsætter informationer om datasikkerhed til en kampagne-video for elever i samme aldersgruppe.

Figur 1: Forløbsmodel for prototyperne



1.1 Beskrivelse

Dette forløb tager udgangspunkt i et nyt færdigheds- og vidensområde, der er hentet fra kompetenceområdet ***teknologisk handleevne*** i faget teknologiforståelse, nemlig ***digital sikkerhed***. Centralt for digital sikkerhed er primært de risici, man kan møde i et digitaliseret samfund, og dernæst hvordan eleverne kan lære at forstå og forholde sig (tage forbehold) – og beskytte sig mod eventuelle trusler. I den eksisterende danskfaglighed er der meget fokus på de kommunikative aspekter af sikkerhedsbegrebet. Her vil teknologiforståelsesfagligheden udvide den eksisterende faglighed med større viden om, hvilke trusler man kan møde i den digitale verden. Det vil give eleverne en øget forståelse for, hvordan de kan handle sikkert og hensigtsmæssigt i den digitale verden.

Formålet med forløbet er at:

- Udvikle elevernes kritiske sans i forhold til egen og andres digitale sikkerhed
- Udvikle viden om, hvad der relevant at være opmærksom på omkring egen og andres digitale sikkerhedsadfærd

Produkt

Eleverne skal igennem en designproces producere en film om digital sikkerhed til andre elever i aldersklassen.

Kriterierne for videoen er, at eleverne skal tegne og fortælle – i øjenhøjde med målgruppen:

- hvordan internettet fungerer
- hvad digitale fodaftryk er
- hvordan vores data bliver overført
- hvordan en cookie fungerer
- hvordan man kan beskytte sig mod trusler og begå sig sikkert

For at komme i øjenhøjde med målgruppen skal der udarbejdes en brugerundersøgelse, som kortlægger, hvor meget målgruppen ved om digital sikkerhed på forhånd.

1.2 Rammer og praktiske forhold

Der skal laves brugeranalyser/spørgeskemaundersøgelser på skolen.
Forløbet er estimeret til at have en varighed på 8-10 lektioner.

1.2.1 Materialer

Forløbet er tilgængeligt på www.tekforsøget.dk

Digitale teknologier

Adgang til Skoletube, hvor eleverne anbefales at bruge WeVideo. Alternativt Powerpoint Mix eller andre præsentations- og video-formater. Eleverne skal til nogle af øvelserne have adgang til enten deres egne eller skolens computere – og de skal til udvalgte øvelser have adgang til egen telefon. Det er en forudsætning, at eleverne har adgang til Firefox og/eller Chrome i udvalgte dele af forløbet.

Elevhenvendte ressourcer (herunder evt. hjemmesideadresser, som ikke findes i ressourcebanken)

Lærerhenvendte ressourcer (herunder evt. hjemmesideadresser, som ikke findes i ressourcebanken)

Lærerressourcerne er lagt ind undervejs.

1.2.2 Lokaler
Undervisningen kan gennemføres i eget klasselokale

1.2.3 Vidienspersoner og andre eksterne aktører
Det kan være en ide at få hjælp fra kollegaer, der tidligere har arbejdet med Wevideo og videoproduktion

1.2.4 Tværfaglighed

2. Mål og faglige begreber
I dette forløb arbejdes der med tre danskfaglige kompetenceområder; læsning, kommunikation og fremstilling. Forløbet har særligt fokus på datasikkerhed, digitalt design og designprocesser fra det teknologifaglige område.

KOMPETENCEOMRÅDER	FREMSTILLING	KOMMUNIKATION	LÆSNING
Kompetencemål	Eleven kan udtrykke sig i skrift, tale, lyd, billede i formelle situationer	Eleven kan deltage reflekteret i kommunikation i komplekse formelle og sociale situationer	Eleven kan styre og regulere sin læseproces og diskutere teksters betydning i deres kontekst
Færdigheds- og vidensmål	Digital design og designprocesser: ▪ Eleven kan gennem konvergente og divergente processer undersøge og analysere komplekse problemfelter og derigennem rammesætte problemstillinger ▪ Eleven har viden om fremstilling med digitale teknologier ▪ Eleven har viden om forskellige argumentationstyper og om udvikling af egen designkompetence	Digital sikkerhed: ▪ Eleven kan handle sikkert og hensigtsmæssigt i interaktionen med digitale teknologier ▪ Eleven har viden om sikkerhedsmæssige aspekter ved færden i den digitale verden	Tekstforståelse: ▪ Eleven kan sammenfatte informationer fra forskellige elementer i teksten ▪ Eleven har viden om metoder til vurdering af teksters formål og perspektiv Sammenhæng: ▪ Kan sætte tekster ind i sammenhæng ▪ Eleven kan kritisk vurdere teksters udsagn på baggrund af kontekst ▪ Eleven har viden om sammenhæng mellem tekst og kontekst

KOMPETENCEOMRÅDER	FREMSTILLING	KOMMUNIKATION	LÆSNING
Færdigheds- og vidensmål	Planlægning: ▪ Eleven har viden om opgave- og problemformulering ▪ Eleven kan organisere samarbejde om fremstilling	Sproglig bevidsthed: ▪ Eleven kan iagttage, hvordan vi danner forestillinger om verden med ord og sprog Krop og drama: ▪ Eleven kan bruge kropssprog og stemme tilpasset kommunikationssituationen IT og kommunikation: ▪ Eleven kan diskutere etiske spørgsmål vedrørende kommunikation på internettet ▪ Eleven kan vælge digitale teknologier i forhold til situationen	

Konkretiserede læringsmål

Vær opmærksom på, at målene i dette forløb ifølge Fælles Mål skal nås efter 9. klasse, hvorfor målene skal tilpasses til elevernes faglige niveau. Herunder fremgår konkretiserede læringsmål for forløbet, som kan danne grundlag for en eventuel yderligere tilpasning af den enkelte lærer inden forløbet gennemføres.

- Eleverne har viden om, hvad der relevant at være opmærksom på omkring egen og andres digitale sikkerhedsadfærd
- Eleverne kan omsætte denne viden i en film, hvorigennem eleverne udviser kritisk sans i forhold til egen og andres digitale sikkerhed
- Eleverne kan anvende viden om design og designprocesser i udviklingen af en film

Centrale (teknologi)faglige begreber

Begrebsoversigten herunder er tænkt som et printet begrebskort (gerne i A3), der kan hænge flere steder i lokalet, så eleverne kan tjekke nogle af de fagbegreber, de møder i materialet undervejs i forløbet:

BEGREB	FORKLARING
Cookie	▪ En cookie er betegnelsen for data, som brugeren har modtaget fra et website på en web-server, og som gemmes hos brugeren, det vil sige i browseren, og senere sendes til samme website, når sitet igen besøges.
Cache	

BEGREB	FORKLARING
	▪ Cachen er et mellemlager i en computer, lommeregner, mobiltelefon, router osv., som processoren bruger til midlertidige beregninger, før de evt. lagres i hukommelsen, f.eks. harddisk eller flash-lager.
Pixeltag	▪ Et pixeltag er en form for teknologi, der er placeret på et website eller i brødteksten i en mail. Pixeltags har til formål at spore bestemte former for aktivitet, f.eks. visninger af et website, når en mail åbnes. Pixeltags bruges ofte i kombination med cookies.
serverlogfiler	▪ En servers automatiske registrering af en sideanmodning, når du besøger et websted. Disse »server-logfiler« indeholder typisk din webanmodning, IP-adresse, browsertype, browsersprog, anmodningsdato og -tidspunkt samt en eller flere cookies, der unikt kan identificere din browser.
Adfærdsrettede reklamer	▪ Datadrevet markedsføring – tillader reklameproducenter at vise reklame og marketing indhold til brugere, som er baseret på deres browser-adfærd.
Browser	▪ Browser
VPN	▪ VPN eller Virtual Private Network, på dansk "virtuelt privat netværk", er betegnelsen for sikker adgang til internettet - en teknik, som anvendes for at skabe punkt til punkt-forbindelser, såkaldte "tunneler", gennem internettet.
Intentionalitet	▪ Den fulde intentionalitet manifesterer sig I det endelige design (artefakt), når valg om funktionalitet, æstetik, form mv. er foretaget.
DSL	▪ DSL står for Digital Subskriber Line, og er en high- speed internet service.
Divergent og konvergent tænkning	▪ Når eleverne arbejder divergent, arbejder de med at udfolde problemfeltet eller udvikle mange ideer samtidig. ▪ Når eleverne arbejder konvergent, arbejder de med indsnævring af problemet eller idéløsning og kvalificering. ▪ Når elever arbejder i designprocesser, benyttes både divergent og konvergent tænkning.
formålsanalyse	▪ Formålsanalyse betegner den proces, hvori et digitalt artefakt undersøges med henblik på at forstå dets funktioner, anvendelsesmuligheder og intention. Formålsanalyse belyser, hvordan en designidé kommer til udtryk gennem fysiske og digitale egenskaber, som for eksempel menuer, knapper og grafiske elementer. Hvor brugsstudier beskæftiger sig med den faktiske brug, kan man sige, at formålsanalyse beskæftiger sig med den tiltænkte brug.
GDPR	▪ EU´s Persondatalov
IP-adresse	▪ Alle enheder, der er forbundet til internettet, tildeles et nummer, der er kendt som IP-adresse (IP= Internet Protokol"). Disse numre tildeles som regel i nationale blokke. En IP-adresse kan ofte bruges til at identificere det sted, hvorfra en enhed skaber forbindelse til internettet – fx der hvor du bor.

3. Forløbsnær del

3.1 Introfase: Forforståelse og kompetencer

I denne fase skal elevers forforståelse for dataprocesser, datasikkerhed og cyperangreb aktiviseres.

3.1.1 Varighed

Varigheden af introfasen er berammet til ca. 5-8 lektioner.

3.1.2 Komplekst problemfelt

I debatten om datasikkerhed og privatliv kommer det ofte til udtryk, at hvis man ikke har noget at skjule, så har man ikke noget at miste. Udsagn som dette kan være udtryk for et uklart billede dels af, hvad data er, dels hvad de potentielle anvendelser er. Desuden kan datasikkerhed forekomme uoverskueligt, fordi brugerne ikke har et klart billede af, hvad de selv kan gøre. De fleste elever har et aktivt liv med digitale teknologier og deler oplysninger om sig selv med de personer, der er i deres netværk. Hvad vi måske ved meget mindre om, er at vi også deler data med de virksomheder, der tilbyder browsere, søgemaskiner, hjemmesider og apps. I dette virvar af lange brugsbetingelser og juridiske paragraffer kan unges viden om digitale rettigheder nemt blive sat på en prøve, og det kan være udfordrende at gennemskue, hvad de giver samtykke eller siger ja til, når de godkender vilkår og betingelser, for hvilke persondata er det reelt, de potentielt deler, når de siger ja? Måske er unge som så mange andre ikke engang helt sikre på, hvad persondata er, og hvad det vil kunne bruges til. Er de overhovedet klar over, at data om dem ofte videregives, når de anvender forskellige digitale tjenester?

3.1.3 Problemstilling

Hvordan informeres unge i aldersgruppen bedst om digital sikkerhed?
Forslag til alternativ: Hvordan lærer unge om de udfordringer og potentielle farer, som eksisterer i forbindelse med digital sikkerhed, når de færdes på nettet?

3.1.4 Iscenesættelse/scenarie:

Opgave 1
Til LÆREREN: Målet med denne øvelse er at få viden om, hvad ordet data betyder. Vi bruger ordet i flæng, men hvad betyder ordet data egentlig? Og i hvilke situationer indgår ordet data? Eleverne skal aktivere deres forforståelse ved at skrive deres eksisterende viden ind i et VØL-skema (vedlagt). VØL-skemaet skal bruges igen i evalueringen af forløbet, så derfor er det vigtigt, at det afleveres på læringsplatformen, så det kan tages frem igen.

Til ELEVEN:

a. Skriv ind i et VØL-skema: Hvad betyder data? Hvor møder du ordet "data"? Hvad kan man oversætte data med (synonymer)? + hvornår afgiver du data? Kan følelser være data? Hvad du gerne vil vide om data?

b. Start med at vise denne video "Hvis din bagerjomfru var en app" https://youtu.be/RdU--d46D80
c. Tag headsets på og lyt til "**Alt er data**", Tryk her (https://youtu.be/-pfWXq2vr-M) af Lone Hørslev og Jesper Mechlenburg.

TIL ELEVEN: Skriv ind i VØL-skemaets første kolonne: Hvad skal happeningen med det skjulte kamera i bagerforretningen vise os om vores data/digitale fodspor?
I digte har alting flere betydninger – mange endda. Man taler om, at et digt har mange lag af betydninger. Hvor mange betydninger kan der ligge i sætningen: "vi forærer det væk" (…) det faktum, at jeg ik kan sige nej, til dig".? Hvad er det, vi forærer væk? Og hvor forærer vi det væk?

Til LÆREREN: Oprindeligt, kommer ordet data fra latin og betyder "**at give**". I mere teknisk forstand kan data oversættes til **information.** Data kan bestå af tal, ord, billeder.

TIL LÆREREN: Mini-fortolkning af "Alt er data" –forfatteren kaster lys på mennesket i et gennemdigitaliseret hverdagsliv, hvor alt dokumenteres online og hvor alt - selv følelser er transformeret til data. "Alt er data – vi forærer det væk" (…) det faktum, at jeg ikke kan sige nej, til dig". Dette tvetydige "dig" kan her enten forstås som et andet menneske eller en cookie, vi møder på en hjemmeside.

Opgave 2: Dit digitale spejlbillede

TIL LÆREREN: Målet med den følgende opgave er, at eleverne skal opnå viden om, at de både **bruger** data, men også **afgiver** data i deres daglige færden. Alle de data, vi efterlader eller giver væk, omtales ofte som **digitale fodspor**. Opgaven går ud på, at hver elev skal konstruere et digitalt spejlbillede af sig selv ved at indsamle alle de synlige persondata og usynlige data, de kan finde ved at undersøge telefonen, Google, snapchat osv. Eleverne får udleveret en skabelon med fem felter, der hver især repræsenterer domæner, som vi dagligt efterlader fodspor i. Det anbefales at printe den i A3, så der er plads til mange forskelligartede observationer. Det er tanken, at hver elev skriver individuelle noter ind (analogt), eftersom undersøgelsen skrider frem. Under arbejdet med de digitale fodspor er det vigtigt at spore eleverne ind på, at det ikke kun er telefonen, der sætter digitale fodspor – Rejsekortet, Sygesikringskortet, skoletandlægen, lægen, Aula indsamler også data om eleverne. Inddel eleverne i grupper eller i makkerpar – i tilfælde af at den ene ikke har en googlekonto eller snapchat.

TIL ELEVEN: I denne øvelse skal du undersøge, hvor mange "steder" du afgiver data - sætter digitale fodspor. Hvornår afgiver du data, og hvilke typer af data giver du væk? Du får nu udleveret en tom skabelon med fem bokse. Den ene boks skal du udfylde med alle de data, du kan finde om dig selv på nettet, på din telefon eller computer. I de andre bokse skal du opliste alle de data som indsamles om dig i de forskellige tjenester, du bruger. Når du har udfyldt skabelonen, ser du et digitalt spejlbillede af dig. Sammenlign med gruppen – makkeren.

a. Hvad ved nettet om dig?
Start med at google dig selv – hvilke informationer dukker op? Brug skabelonen og noter, hvad du finder.

b. Hvad ved mine omgivelser om dig? Du skal nu udfylde den del af skabelonen, som handler om dine digitale fodspor i hverdagen. Tænk en gennemsnitlig dag igennem – og gennemgå dine daglige rutiner for digitale fodspor: når du står op, når du tager bussen/toget i skole, når du går forbi steder, der er kameraovervåget? Hvilke data afgiver du, når du går ind på skolens område – når du går til på skolens digitale platform Aula, når du går til skoletandlæge, sundhedsplejerske, når du betaler med betalingskort osv.

c. Hvad ved din telefon om dig? Gå ind på din telefon og undersøg, hvilke data dine apps henter om dig fra din telefon. Hvis du har en IPhone, skal du søge under, "Anonymitet", hvis du har en Android skal du se under privatlivsindstillinger. Noter hvilke data de forskellige apps har adgang til, fx.:

Hvilke apps har adgang til din mikrofon
Hvilke apps har adgang til din lokation
Hvilke apps har adgang til dit kamera
Hvilke apps har adgang til dine kontakter
Hvilke apps har adgang til dine fotos
Hvilke apps har adgang til dine sms´er

d. Hvad ved Google om dig? I din liste over digitale fodspor skal du skrive, hvad Google ved om dig – hvis du har en googlekonto. Du kan se din søgehistorik her: https://myactivity.google.com/myactivity. Noter de sidste par dages søgehistorik, hvad du har besøgt, og hvornår du har besøgt de forskellige sider. Og du kan i dette link se, hvad Google gætter på om dig og dine interesser her: https://adssettings.google.com/u/0/authenticated

e. Hvad ved Snapchat om dig? privatlivspolitik Klik her: https://www.snap.com/da-DK/privacy/privacy-policy/ - i afsnittet "Kontrol over dine data" har du mulighed for at "Downloade mine data". Når du klikker her, får du vist en liste over de data, du kan få adgang til – og de data, som Snapchat gemmer om dig – som du IKKE kan få adgang til. Klik her: https://accounts.snapchat.com/accounts/downloadmydata

3.1.5 Fagligt loop

Slut af med at se filmen: CTRL over dine digitale spor her: https://youtu.be/5iz5yVrC-kg

Se denne video om, hvordan du færdes mere sikkert med din telefon: Digitalt selvforsvar (https://youtu.be/t0JGcnx5PnM)

Se inspirationsvideoer på denne side: https://emu.dk/grundskole/it-og-teknologi/cybersikkerhed/inspirationsvideoer

3.1.6 Fagligt Loop

Opgaveforløbet sluttes af med et spil med spørgsmålskort fra Medierådet (se vedlagte materialer). Eleverne skal sammen i grupper af fire igennem en researchproces, hvor de skal undersøge forskellige aspekter af datasikkerhed og hvordan man beskytter sig selv mod cybertrusler. Den viden, som de får ud af researchen, skal de bruge aktivt i deres video-produktion: datasikkerheds-kampagne til jævnaldrende elever. Klassen deles op i researchgrupper á 3-4 elever Grupperne får tildelt et nummer fra 1-5, svarende til emneinddelingen herunder. Eleverne kan finde svar på deres spørgsmål i disse inspirationsvideoer: https://emu.dk/grundskole/it-og-teknologi/cybersikkerhed/inspirationsvideoer'

Formalia: Alle grupper forbereder et mini-foredrag på 10 minutter om deres emne. Grupperne understøtter deres formidling med 5-6 slides i en PPT.

Emneinddeling:

1: Lytter SIRI med?
2: Hvad er en cookie?
3: Du bliver, hvad du liker.
4: Hvordan undgår man at blive snydt på nettet?
5: Sådan bliver du en haj til datasikkerhed

GRUPPE 1: Lytter SIRI med?

1: I skal forklare resten af klassen, om det er fup eller fakta, at facebook lytter med sådan som videoen påstår? Se udsendelsen: Siri lytter med (11 minutter): https://youtu.be/euAjehjjBW4
Find mere viden i artiklen – "Det løb løber koldt ned ad ryggen" fra Politiken

2: I skal forklare, hvad "målrettede reklamer er". Find eksempler på situationer, hvor I har oplevet målrettede reklamer på internettet. Måske har I været på H&M eller Boozt, Zalando, og opdager, at de sko I kiggede på, dukkede op på andre internetsider efter flere dage? Målrettede reklamer kan altså dukke op på en anden webside, som ikke havde noget med den oprindelige søgning at gøre. Giv eksempler. Giv en forklaring på, hvordan målrettede reklamer bliver skabt.

GRUPPE 2: Hvad er en Cookie?

1: I skal forklare resten af klassen:

a. hvad er en cookie?
b. Hvor møder vi cookies?
c. Hvordan fungerer en cookie?
d. Hvad sker der, hvis man trykker "nej" til en cookie?
e. Hvad bliver en cookie brugt til?

I kan finde viden i Forbrugerrådet TÆNK: https://taenk.dk/test-og-forbrugerliv/digitale-tjenester/cookies-bestemmer-dine-reklamer

Supplerende læsning: Læs "hvad er en cookie" og "Hvad bliver cookies brugt til":
https://cookieinformation.com/da/videnscenter/blog/hvad-er-en-cookie
Red Barnet her: https://redbarnet.dk/skole/sikkerchat/ctrl-over-dine-digitale-spor/

GRUPPE 3: Du bliver, hvad du liker

I skal forklare resten af klassen, hvorfor I får forskellige resultater, når I søger på nettet – og hvordan man kan slette data, der gemmes i browseren:

a. tag jeres mobiler (eller computer) frem – og lav en søgning i browseren. Det skal være identiske browsere, I bruger. Den søgning I laver, skal også være identisk – f.eks. hvordan laver man snobrød eller hvad er en influencers fulde navn, "hvor bor julemanden" osv.' Forklar, hvorfor får I forskellige hits? Brug evt. denne video som kilde: "Det skræddersyede Internet": https://youtu.be/MSw6Flu2coQ

b. Læs "Du er varen" og "Algoritmer, - du bliver´ hvad du liker" se teksten her: https://indd.adobe.com/view/8d91fa8e-6b2a-47e0-b0c9-429d89df2737?startpage=6 - og giv en forklaring på, hvorfor vi får forskellige søgeresultater, når vi søger på det samme ...

Hjælp dine klassekammerater med at slette data, der gemmes i browseren - tryk CRL +H, eller tjek linket her: https://support.google.com/chrome/answer/95589?co=GENIE.Platform%3DDesktop&hl=da-DK

GRUPPE 4: Hvordan undgår man at blive snydt på nettet?
I skal forklare, hvordan I undgår at blive snydt på nettet

a. Webshops gør det let at købe varer hjemme fra sofaen. Men er netbutikken sikker og pålidelig, eller risikerer du at miste dine penge uden at få din vare? Det kan være svært at gennemskue, hvis man ikke ser sig godt for. Formulér 4-5 gode råd. Inddrag linket her: https://taenk.dk/raadgivning-og-rettigheder/online-shopping/onlineshopping-saadan-handler-du-sikkert

b. Hvordan kan man vide, om den side man befinder sig på, er en sikker webside? Kik her og lær om symbolerne for en sikker forbindelse: https://support.google.com/chrome/answer/95617?hl=da

   Forklar, hvad et sikkerhedscertifikat er og hvordan man kan bruge den til at undgå at blive snydt på nettet.

GRUPPE 5: Sådan bliver du en haj til datasikkerhed.

I skal forklare resten af klassen, hvordan man beskytter sig på nettet:

a. Før I går i gang, skal I besøge denne hjemmeside hos virksomheden Kaspersky, som leverer digitale sikkerhedstjenester: https://cybermap.kaspersky.com/ - klik på et par lande og se, hvor stor risikoen for cyperangreb er.

b. I jeres mini-foredrag skal I forklare, hvad Inkognito er. Herunder får I nogle ledetråde: Inkognito er en privat-indstilling i browseren, som tillader at browse, uden at efterlade spor i søgehistorik, browserhistorik, downloadhistorik. I det hele taget gemmer browseren ikke på oplysninger om din internetfærden, når du bruger den private funktion Incognito. Du finder den ved at højreklikke på Chrome ikonet og vælger nyt-inkognito-vindue.

c. Download evt. appen "Mit digitale selvforsvar" – og udvælg nogle gode råd fra appen, som I synes er vigtige og som skal med i jeres mini-foredrag.

3.2 Udfordrings- og konstruktionsfase

3.2.1 Varighed

Forløbet er estimeret til at have en varighed på 7 lektioner.

3.2.2 Faglige loops

Eleverne skal komme med ideer til en videoteaser (fx. Imovie-forfilm), tegn- og fortæl-video, animation, stop-motion, skærmoptagelser eller andre formater, der skal gøre eleverne i ca. samme aldersgruppe – interesserede i digital sikkerhed og persondata. Dette gøres gennem en idegenereringsproces med

feedback-loops. I designprocessen opfordres eleverne til at lader sig inspirere af "Siri lytter med" og CTRL-videoer fra Red Barnet, hjemmesider (click click) og på baggrund af disse genererer ideer til:

1: hvordan gør vi andre unge interesserede i datasikkerhed?
2: hvad ved vi om modtagerne – målgruppe, alder, interesse, viden (modstand)
3: hvordan bryder vi modstanden (hvis der er nogen)?
4: hvilken videogenre/format skal vi bruge?
5: Hvilke modaliteter skal vi integrere?

Herefter skal eleverne udarbejde en tegnet mockup/drejebog (skabelon bliver vedlagt) - hvor de angiver, hvilke multimodale udtryk i form af billeder, symboler og tegn, de har tænkt sig at bruge. I denne fase er det legitimt at genbesøge og finde inspiration i nogle af de sites, som blev brugt i intro-forløbet. Eleverne arbejder i iterative faser med feedback-loops – med henblik på at forfine produktet i forhold til de æstetiske og adfærdsdesignmæssige udtryk.

Eleverne giver feedback på drejebogsniveau og de får de mulighed for at øve sig i at argumentere for deres valg/fravalg, men også i at modtage feedback med henblik på at kvalificere designet.
Mock-uppen7drejebogen kan være kreativt og håndgribeligt (papir, printede billeder osv..).

- Præsenter ideen/pitch ideen for hinanden
- Kom med forslag til løsninger, vis fx nogle af designelementerne i form multimodale udtryk og effekter.
- Italesæt, hvad den ønskede effekt potentielt skal være

Feedback-loop
Sæt eleverne sammen i produktionsgrupper og tal om, hvordan man giver feedback på hinandens drejebøger. Formuler i fællesskab de nysgerrige spørgsmål, som de kan stille til hinandens ideer til løsningerne fx

- Hvem skal informeres?
- Hvad ved vi om dem, der skal informeres?
- Hvad ved de om området i forvejen?
- Hvilke virkemidler skal der bruges og hvorfor?
- Kan de der skal se videoen – og har det den ønskede effekt? Hvorfor/ hvorfor ikke?

Revision af designforslagene. Evt. en ny præsentation.

Spørgeskemaundersøgelse – hvad ved dine kammerater om digital sikkerhed?
inspirationsloop:

Denne video findes på siden "Rådet for digital Sikkerhed" –børnene, der optræder, bliver spurgt om, hvad "digital" eller "digitalisering" betyder. Se videoen her. (https://vimeo.com/167779785)

Hvis der er tid – kan det anbefales, at eleverne laver en spørgeskemaundersøgelse, hvor de interviewer 3-4 elever på skolen. Formålet er at få en forståelse for, hvad målgruppen ved –og deres erfaring med cypersikkerhed

- Hvad er digitale fodspor?
- Hvordan laver man digitale fodspor?
- Hvad er en cookie? Forklar, hvordan den fungerer.
- Hvad betyder ordet samtykke?
- Når du trykker okay for en cookie – hvad giver du så udbyderen lov til?
- Vidste du, hvilke data du har givet Instagram og/eller Facebook adgang til, før du downloadede appen?
- Er Messenger et lukket og privat forum?
- Hvad er VPN?
- Hvor mange apps har adgang til din lokalitet på din telefon?
- Har du altid bluetooth slået til på din telefon?
- Hopper du på offentlige netværk, når du er på ferie?
- Hvordan ser du forskel på sikre og usikre sider på nettet?
- Hvad er GDPR?

TIL LÆREREN: eleverne kan enten besvare spørgeskemaet individuelt (Her vil det så være læreren, der samler svarene ind fx i Google Analyse), eller eleverne kan indsamle svar fra andre elever (3-4 stk.), som de tilfældige møder på skolen – fx i frikvarteret. I opsamlingen på en padlet med 7 kolonner skal eleverne angive svar fra elever, der interviewede. Eleverne skal herefter forsøge at samle konklusionerne. Her kan de både tænke i, hvilke svar der går igen, og hvilke svar der er overraskende eller anderledes. Undersøgelsen skulle gerne være med til at pointere, hvad undersøgelser også viser: at vi meget sjældent ved ret meget om datasikkerhed og privatliv:

3.3 Outrofase: Ny forståelse og nye kompetencer

3.3.1 Varighed

Varigheden er estimeret til at være 1-2 lektioner

3.3.2 Fremlæggelse og introspektion

Eleverne opfordres til at tage deres VØL-skemaer frem og udfylde den sidste del. Herefter deler eleverne deres skema med hinanden to og to og snakker om, hvad de har været igennem i forløbet. Når de har delt, hvad de har skrevet, så skal de beslutte, hvilke pointer som skal deles med klassen.

4. Perspektivering

4.1 Evaluering

I perspektiverings- og efterbehandlingsfasen er det væsentligt at vende tilbage til det komplekse problem.
Hvilke forståelser er der opstået hos eleverne?
Hvilke begreber har de taget til sig, forstår de dem?
Der lægges op til en evaluering i brugen af de billeder og tekster, som eleverne har skrevet. Det kan fx gøres ved, at designprocessen fastholdes via billeder, lyd og video i BookCreator. Outrofasen kan være væsentlig at fastholde vigtige tegn på refleksion hos elever over begrebet automatisering, men også i forhold til den digitale myndiggørelse.

4.2 Progression

I dansk i udskoling skal elever arbejde frem mod at kunne strukturere og gennemføre en proces med produktion af større multimodale produkter. Det er et fagligt område, som eleverne anvender i mange sammenhænge og som kan benyttes i projektopgaven. I arbejdet med video i forløbet bliver danskfagligheden suppleret med faglighed fra teknologiforståelse. I et forløb med fokus på at fremstille et større multimodalt produkt er det oplagt at indarbejde den iterative proces fra teknologiforståelsesfagligheden, hvor eleverne afprøver, fejler og justerer deres proces og produkt.

4.3 Differentieringsmuligheder

Gruppeøvelserne give gode muligheder for at differentiere. Både internt i grupperne, hvor de stærke elever kan tage ansvar for de sværeste opgaver, men også mellem grupperne, hvor de dygtige grupper kan nå længere med deres opgave. Det er vigtigt, at eleverne gennem de faglige loops får en forståelse af, at de arbejder med en proces, som hele tiden kan forbedres. Gennem feedback loops bliver de hele tiden udfordret til at stille spørgsmål og finde bedre løsninger. Hurtige grupper kan opfordres til at gennemgå flere loops.

4.4 Særlige opmærksomhedspunkter

Inden forløbet påbegyndes, beder vi dig om at læse opgaverne igennem med henblik på at overveje, hvornår du vurderer dine elever, er sikre eller usikre. Du skal tænke det sådan, at eleverne kan være sikre eller usikre ift. fagligt indhold, men også i forhold til den proces, som eleverne skal igennem. Nogle elever er måske udfordrede i det seancer, hvor elevstyringen er høj og lærerstyringen lav og omvendt, og her kan de have særligt brug for stilladsering af enten ekstra opgaver, lærerstilladsering eller pararbejde mv.