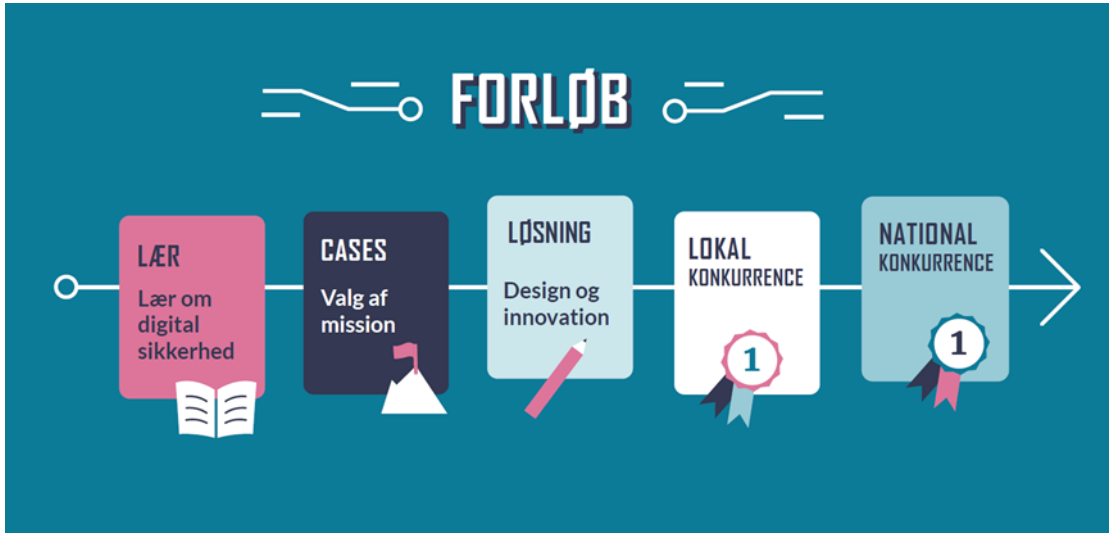
Lærervejledning

Dét skal du vide før du går i gang

Denne konkurrence er tænkt som et fagligt undervisningsforløb på ca. 10-15 lektioner. Målgruppen er mellemtrinnet (4.-6. klasse) og forløbet retter sig mod flere fag; dansk, matematik, teknologiforståelse (pt. prøvefag på 46 skoler) samt det tværgående tema it og medier. Derudover kan man med fordel indtænke håndværk og design i design- og innovationsfasen, når eleverne skal producere og præsentere deres løsning. Det er eleverne, som er de aktive i konkurrencen. Gennem innovation og idégenerering skal de skabe løsninger, der imødekommer missionernes krav og udfordringer.

Har du tilmeldt dig konkurrencen, får du tilsendt et missions-kit, som består af begrebs- og øvelsesplakater, diplomer og klistermærker, der understøtter forløbet og bidrager til at fastholde opmærksomheden på det lærte - også efter at konkurrencen er slut.

Forløbsplanen ser sådan ud:



CYBERMISSIONEN

Inspirationsmateriale, cases og missioner

Konkurrencen tager udgangspunkt i fire aktuelle cases, som omhandler it-sikkerhed og databeskyttelse i børnehøjde. Hertil knytter sig nogle missioner, som eleverne skal løse.

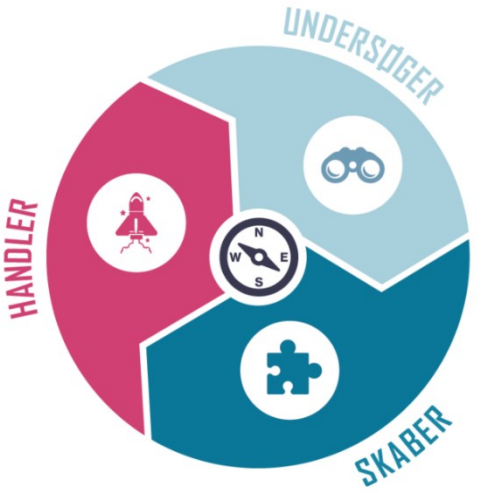
I forløbet arbejder I med et inspirationsmateriale, hvor eleverne lærer om grundlæggende it-sikkerhed, får bedre styr på deres digitale sikkerhed og får en forforståelse, som de skal benytte, når de skal udvikle løsninger på missionerne.

Målet med forløbet er, at eleverne efter 10-15 lektioner har kendskab til:

- grundlæggende begreber i forhold til digital sikkerhed
- hvordan de efterlader 'digitale spor', som andre kan (mis)bruge, og hvorfor man skal være opmærksom på det
- hvordan de kan beskytte sig mod hacking og misbrug af deres konti.

Designproces

Når eleverne har tilegnet sig grundlæggende viden om digital sikkerhed gennem inspirationsmaterialet, er blevet præsenteret for de forskellige cases og har valgt én mission, så skal de igennem en innovations- og designproces. Her skal de bruge den viden, som de har fået i de første lektioner - samt deres opfindsomhed - til at finde løsninger på missionerne.



Innovations- og designmodellen er bygget op omkring tre faser, hvor eleverne skal:

- undersøge problemstillingen fra deres valgte mission og sætte sig i målgruppens sted
- finde på idéer til løsninger og udvælge én løsning, der udvikles på
- designe en løsning samt evt. en prototype

Hvordan skal løsningen præsenteres?

Eleverne skal fremlægge deres løsningsforslag i et pitch, dvs en kort præsentation, hvor skal de redegøre for missionen, fortælle om deres proces med at finde frem til løsningsforslaget samt præsentere selve løsningsforslaget. Der er ikke krav til formatet på løsningsforslaget; det kan være en kampagne til hele skolen, en quiz, en lille oplysningsfilm, en app eller noget helt andet, som kun elevernes fantasi sætter grænsen for. Der forventes ikke nødvendigvis et helt færdigudviklet produkt. Det er processen, kreativiteten samt at løsningsforslaget afspejler, at eleverne har tilegnet sig en viden om it-sikkerhed, der er det afgørende.

Hvordan nominerer man sig til konkurrencen og hvordan sendes løsningen?

Hver klasse må max sende ét løsningsforslag ind til dommerpanelet. Derfor foreslås det, at klasserne holder deres egne lokale konkurrencer, hvor eleverne præsenterer deres løsningsforslag på klassen eller for et dommerpanel, som hjælper med at finde det bedste løsningsforslag, som sendes ind til den nationale konkurrence. Det lokale dommerpanelet kan bestå af skolelederen, skolebestyrelsesformanden, PLC-person og/eller skolens IT-vejleder. Når klassen eller skolen har fundet det bedste løsningsforslag, skal præsentationen optages og uploades af den tilmeldte lærer på Cybermissionens side på emu.dk. Herefter vurderes alle de indkomne videopræsentationer, af et dommerpanel bestående af de cybermissionsansvarlige i Styrelsen for It og Læring og repræsentanter fra Rigspolitiets Nationale Cybercrime Center.

Præsentationerne vurderes ud fra følgende kriterier:

- eleverne har gennemført den valgte mission
- eleverne demonstrerer relevant viden om digital sikkerhed og kan bruge fagudtryk
- eleverne fremlægger deres problemstilling, research, designvalg og løsning klart og præcist, og de har forskellige produkter med, som understøtter deres formidling
- eleverne har lavet en original og troværdig løsning, hvor sammenhængen mellem deres research og missionens problemstilling er klar.

Muligheden for at uploade/indsende videoer til den nationale konkurrence åbner den 23. november.

Vi opfordrer til, at forældrene orienteres om konkurrencen og om, muligheden for at eleverne, som en del af undervisningen optræder i en video, der sendes ind til ministeriet og Rigspolitiet. Vær opmærksom på, at når eleverne er under 15, er forældrene det databeskyttelsesretlige subjekt og derfor er det dem, der skal godkende at videoer, hvor deres børn deltager sendes ind til konkurrencen.

Videoerne vil efter upload ikke blive offentliggjort og er udelukkende synlige for udvalgte personer i STIL og hos Rigspolitiet. Vinderne af konkurrencen vil blive kontaktet særskilt og spurgt om tilladelse forud for en eventuel offentliggørelse af deres video.

Forslag til lektionsplan

Viden om digital sikkerhed	
Varighed	2-3 lektioner
Mål	At eleverne får basal viden om digital sikkerhed, så de kan forstå de problematikker, der knytter sig til digital sikkerhed samt et udgangspunkt at arbejde ud fra, når de skal innovere og idégenere ud fra deres valgte mission. At eleverne får en begrebsafklaring af "Digital sikkerhed"
Aktiviteter	På emu.dk ligger der under temaerne Cybersikkerhed og Digital dømmekraft en mængde materiale, som kan benyttes til en indføring i emnet om digital sikkerhed. Der findes bl.a. forløb og konkrete aktiviteter, som er målrettet mellemtrinnet. Derudover foreslås det, at indlede forløbet med at gennemgå begrebsplakaten i det tilsendte missions-kit, så eleverne har forståelse for de centrale begreber inden for it-sikkerhed og databeskyttelse. Plakaten kan også printes på emu.dk. Eleverne skal undervises i sondringen mellem "Dine data i verden" og "Dine personlige konti": **"Dine data i verden'** dækker over den opmærksomhed, man bør have på, at vi alle sætter digitale fodspor hele tiden, når vi er online og bruger apps og tjenester, og at denne data bliver brugt, solgt videre og er tilgængelig for rigtig mange mennesker og firmaer. Det er ikke ligegyldigt, hvor og hvad man lægger ud, og hvad man siger ja til. Man kan øge sin bevidsthed om dette. Her foreslås det, at anvende øvelsesplakaten om digitale fodspor i det tilsendte missions-kit. Plakaten kan også printes på emu.dk. **'Dine personlige konti'** er basal beskyttelse af noget af det vigtigste og mest personlige, mennesker har i dag: Adgangen til de konti, man har på de mange tjenester, man bruger. Konsekvenserne af andres adgang hertil kan være uoverskuelige og ødelæggende. Tænk almindelig sund omgang med fx passwords.

	På Cybermissionens side, kan du også finde links til øvrige gratis undervisningsmaterialer om it-sikkerhed og databeskyttelse som du med fordel kan inddrage i forløbet.
Præsentation af missioner	
Varighed	1-2 lektioner
Mål	At eleverne får indblik i konkrete problematikker fra den virkelige verden, som de kan relatere til deres eget liv. At eleverne forstår, at der er nogle konkrete problematikker knyttet til digital sikkerhed, og at de i grupper udvælger én mission at arbejde ud fra.
Aktivitet	De aktuelle cases gennemgås og vendes på klassen. Herefter skal eleverne, i grupper, læse missionerne og sammen drøfte de arbejdsspørgsmål, som er knyttet til dem. De skal herefter udvælge hvilken mission, de vil arbejde videre med. Når eleverne har valgt mellem de forskellige missioner (eller måske lavet deres egen) er de klar til innovations- og designproces.
Innovations- og designproces	
Varighed	6-8 lektioner
Mål	At eleverne gennemgår en innovations- og designproces hvor de bruger deres viden og opfindsomhed til at finde på løsninger på problemstillinger, der knytter sig til digital sikkerhed.
Aktiviteter	**Fase 1. Eleverne undersøger problemstillingen i deres valgte mission.** Her kan de bl.a. benytte sig af øvelsen De Bonos seks tænkehatte, hvor de indtager forskellige positioner ift. problemstillingen. Idéen med hattene er, at du bliver en anden, når du tager en hat på. Hvis du f.eks. arbejder med en case om datadeling på sociale medier, vil du med den gule hat på være optimistisk og dermed ikke mene, at det er et stort problem at lægge noget på de sociale

	medier. Har du i stedet den røde hat på, fortæller du om de følelser, som casen skaber hos dig; at du fx føler dig nervøs og overvåget på sociale medier. Du kan også forestille dig, at du er forældre til et barn, der er på TikTok og er bekymret for, hvad dit barn deler der. Her er det den sorte hat, som du tager på og taler ud fra. Det er ikke nødvendigt at bruge alle hattene. Men det er afgørende at bruge én hat ad gangen. Hver hat har en farve og en værdi.  **Fase 2: Eleverne finder på idéer til løsninger og vælge én.** Eleverne kan lave en brainstorm over idéer til, hvordan de vil løse deres mission. De kan lade sig inspirere af materiale på emu.dk eller selv søge andet relevant materiale. De kan også her prøve at sætte sig interessenternes sted og overveje, hvilke løsninger de ville foretrække. Til sidst skal de vælge én løsning, som de vil arbejde videre med.

	Fase 3: Eleverne designer løsninger Nu skal eleverne designe deres løsning og evt. en prototype, hvis det er muligt og løsningen lægger op til det. Denne fase tager ofte lang tid og kan kræve, at eleverne må starte forfra med nye idéer, hvis den valgte idé viser sig at være svær at udføre. Når eleverne er færdige med løsningsforslaget, skal de øve deres pitch, dvs. hvordan de vil præsentere deres løsningsforslag for de øvrige elever i klassen eller på skolen.
Pitch og konkurrence	
Varighed	2-4 lektioner
Mål	At eleverne lærer at lave en kort pitch, hvor de redegør for deres problem, idé og løsning.
Aktivitet	Eleverne planlægger deres pitch som skal tage ca. 5 min. En typisk pitch falder i 3-4 dele: indledning, præsentation af problem, løsning og evt. hvordan de er kommet frem til den. Det kan være en rigtig god idé at have nogle dommere med, som ikke er klassens nære lærere. Måske skolelederen, elevrådet, en bekendt, en lærer fra et andet trin eller andre vil stille op. Når alle grupper har fremlagt kåres én af klassens løsninger, som optages og sendes til den nationale konkurrence. Videoen må max være 5 min lang.

Cases	
Case : Beskyt dine password	
	Man har passwords eller adgangskoder på alle ens personlige konti: Unilogin, sociale medier, computer, tablet, mobiltelefonen. Det er lidt ligesom at have lås på ens dør derhjemme eller lås på sin cykel. Politiet har lagt mærke til, at børn nogle gange deler deres passwords med hinanden som et bevis på, at de stoler på hinanden og er meget gode venner. Derudover oplever Politiet også, at der bliver delt passwords, når venner hjælper hinanden med at opretholde hinandens streaks på Snapchat. Faktisk gælder det ikke kun børn, en undersøgelse fra 2018 viser, at 38% deler deres personlige passwords med deres partner, familie eller venner. Til casen knytter sig følgende mission(er): **Mission: Pas på dine passwords**

Case: Dine data på nettet

Den populære app og sociale netværkstjeneste TikTok, hvor brugere deler korte videoer med sang-efterligning, humor, dans eller på anden vis viser deres talenter, har fået alvorlig kritik for deres dataindsamling og problemer med sikkerheden. Datatilsynet, der rådgiver og vejleder og gennemfører tilsyn med myndigheder og virksomheder, har derfor besluttet at indlede en undersøgelse, om hvorvidt TikTok overholder GDPR-forordningen. Læs mere om sagen her.

Til casen knytter sig følgende mission(er):

- **Mission: Digitale fodspor**
- **Mission: CTRL your Cookies**

Faktaboks: Persondataforordningen (eller GDPR) er et sæt regler for myndigheder, organisationer og virksomheder, der opbevarer data om personer som f.eks. ansatte, kunder eller brugere. Reglerne indeholder en række krav til, hvordan de skal passe på disse data. Reglerne er til for, at personer, der afgiver deres data, er sikre på, at myndigheden, organisationen og virksomheden passer ordentligt på dem og ikke med- eller modvilligt videregiver dem til uvedkommende parter. Uretmæssig videregivelse af data er nemlig det mest grundlæggende brud på GDPR. Mange af de regler, man ser med den nye persondatalov fra maj 2018, eksisterede også før loven trådte i kraft. Der er dog to store forskelle: der er nu risiko for store bøder, hvis virksomheder og organisationer m.v. ikke overholder persondataforordningen. Derudover skal virksomheder nu forklare, hvad de gør med dine data, og du skal sige ja til, at de må bruge dataene.

Case: Aimbot rammer mere end det, du sigter på

Måske har du oplevet, at én person du ikke kender, har skrevet til dig på Snapchat, i Fortnite eller et andet online spil eller socialt medie? Eller måske har du oplevet, at en person ikke er den, som han eller hun udgiver sig for at være?

Bag skærmen er der nogle, som udnytter, at man kan være anonym til eksempelvis at lokke personlige informationer ud af dig eller få adgang til din computer eller tablet. Eksempelvis er det kendt af politiet, at hackere bruger spilplatforme som Sims, Roblox, Minecraft, Fortnite og andre til at komme i kontakt med børn og unge. De udgiver sig typisk for at være en jævnaldrende medspiller og sender herefter et link til en side, hvor man fx kan downloade et snydeprogram, som giver adgang til alle baner i spillet eller som sikrer, at man rammer, hver gang man sigter på fjenden. Det kan jo være fristende. Men i mange tilfælde vil man sammen med snydeprogrammet også downloade et usynligt program, som giver hackere adgang til at se alt, hvad der foregår på computeren. Det vil sige, at de eksempelvis kan overvåge alt, hvad du foretager dig på computeren, stjæle dine og din familiens passwords, billeder og andre oplysninger og dermed få adgang til bankkonti, sociale medier mm. Derfor er det vigtigt ikke at klikke på links eller downloade programmer uden at tale med en voksen først.

Til casen knytter sig følgende mission(er):

- **Mission - Ansigtsløs kommunikation**

Case: Ansigtsløskommunikation – hvem snakker vi med, når vi er online?	
	På sociale medier og i spil er det nemt og sjovt at få nye venner og møde nogle med de samme interesser, som dig selv. Men desværre findes der også voksne på nettet, som prøver at snyde børn og få dem til at gøre ubehagelige ting. Dem kalder man 'groomere' og de er en slags digitale børnelokkere. Typisk udgiver en 'groomer' sig for at være en anden person, når de er online. Eksempelvis kan en "groomer" være en voksen person, som udgiver sig for at være en jævnaldrende, som skriver til dig online. Efterhånden som jeres kommunikation udvikler sig, vil "groomeren" måske lokke dig til at sende nøgenbilleder eller gøre andre ubehagelige ting. Til casen knytter sig følgende mission(er): • **Mission - Ansigtsløs kommunikation**