



CYBERMISSION 3

DATA: BRUG OG

BESKYTTELSE



BØRNE- OG
UNDERVISNINGSMINISTERIET
STYRELSEN FOR
UNDERVISNING OG KVALITET





**CYBERMISSION 3 - DATA: BRUG OG
BESKYTTELSE**

Design:
Børne- og
Undervisningsministeriet

Børne- og Undervisningsministeriet
Styrelsen for It og Læring
Vester Voldgade 123
1552 København V

© Børne- og Undervisningsministeriet 2021





CYBERMISSION 3 - DATA: BRUG OG BESKYTTELSE

Vi bruger internettet og dets muligheder i vores dagligdag. Vi er for det meste ikke kritiske i brugen af sociale medier, digitale assistenter m.m., der kan udnyttes af andre.

Når vi deler vores adresse på Facebook, når vi har skrevet en fødselsdato på Instagram og vores telefonnummer ligger på skolens webside, så er der i visse tilfælde personoplysninger nok til, at en cyberkriminal kan bryde ind i vores mailboks eller på anden vis få adgang til ens personlige oplysninger.

IT-SIKKERHED ER IKKE ALTID LIGE SJOV!

Det kan være tidskrævende at skulle sige nej tak til cookies og sende personlige oplysninger til venner og bekendte på en e-mail. Det er bare lettere at bruge de sociale medier som kommunikationsplatform og acceptere cookies for at komme hurtig videre.

Når vi anvender Facebook, Instagram, G-mail osv. så betaler vi med vores data – eksempelvis vores personoplysninger, og virksomhederne bagved kan bruge de data til at sende målrettede reklamer. Men data, kan også bruges til at manipulere forbrugerne via målrettet propaganda eller fake news, som det eksempelvis kom frem i Cambridge Analytica-sagen.

VI SKAL PASSE BEDRE PÅ VORES PRIVATE DATA!

Databeskyttelse er vigtigt, og derfor har EU indført Persondataforordningen, der skal sikre, at vi har mulighed for at vælge, hvem vi vil dele personlige data med.

På denne mission skal I arbejde med anvendelse af privat data. I skal også skabe et overblik over, hvad man kan gøre for at være lidt mere privat online og blive bedre til at passe på egne data. I skal både udarbejde en plakat, lave et dataflow-diagram og forberede en præsentation af jeres løsning.

JERES MISSION

På mission 3 skal I vælge ét eller begge temaer herunder. I grupper skal I lave en plakat, der fokuserer på det valgte tema. I skal tage udgangspunkt i målgruppen unge mellem 15-25 år, hvoraf halvdelen i 2020, ifølge Danmarks Statistik, har oplevet sikkerhedsproblemer.

TEMA 1

SÅDAN SPREDES DATA, NÅR I ER ONLINE

Lav en plakat, der viser, hvordan forskellige typer af privat data sendes fra en web-side til en web-shop, hvorefter data måske sælges til en masse firmaer, og bliver brugt på anden vis, end man måske tror.

Udover plakaten skal I lave et dataflow-diagram. I kan lave et dataflow-diagram over, hvad der sker med de data, man deler på Instagram, TIKTOK eller Facebook. Hvad sker der med ens data, når man skriver eller uploader fx en video eller et billede? Og hvad sker der, hvis man deler noget, som andre har lavet? Det kan også være et diagram over, hvad der sker, hvis man bruger sin stemme og beder Siri eller google assistenten om at købe en pizza. Hvor sendes data hen, og hvem bruger det til hvad?

TEMA 2

DET SKER DER, NÅR DU SIGER JA TIL COOKIES

Lav en let forståelig plakat, der viser målgruppen, hvad der sker, når man siger ja eller nej til cookies. I skal derfor bruge tid på at undersøge, hvad en cookie reelt er, og hvad de forskellige typer af cookies kan gøre.

Ud over plakaten skal I udvælge en hjemmeside og finde ud af, hvad det er for en type af cookies, hjemmesiden sætter på jeres computer/telefon, hvis I klikker "accepter cookies". I skal finde ud af, hvad der sker med jeres data og lave et tilhørende dataflow-diagram.

INSPIRATION

For at løse denne cybermission har vi udarbejdet tre oplæg med relevante virksomheder, som vil hjælpe jer til at forstå missionen og give jer bedre indsigt i begreberne og værktøjerne. Vi anbefaler, at I ser alle tre videoer, inden I begynder på missionen. Videoerne varer mellem 8-12 minutter.

Videoerne til **CYBERMISSION 3 - DATA: BRUG OG BESKYTTELSE** finder I her: <https://cybermissionen.cyberskills.dk/mission-3/>

Video 1)

Hvorfor skal vi blive bedre til at passe på egne data?

Video 2)

Hvad er cookies?

Video 3)

Sådan laver du et godt dataflow-diagram

METODER

I det følgende finder du tre forskellige værktøjer, der kan hjælpe jer med missionen:

1. Sådan laver du den gode plakat
2. Sådan laver du et dataflow-diagram
3. Sådan finder du viden om cookies

1. DEN GODE PLAKAT

Plakaten skal formidle problemstillingen overfor målgruppen. Den kan indeholde billeder, tekst, fakta eller noget helt andet til at beskrive, det I ønsker at kommunikere. I kan lave flere plakater, hvis I har lyst.

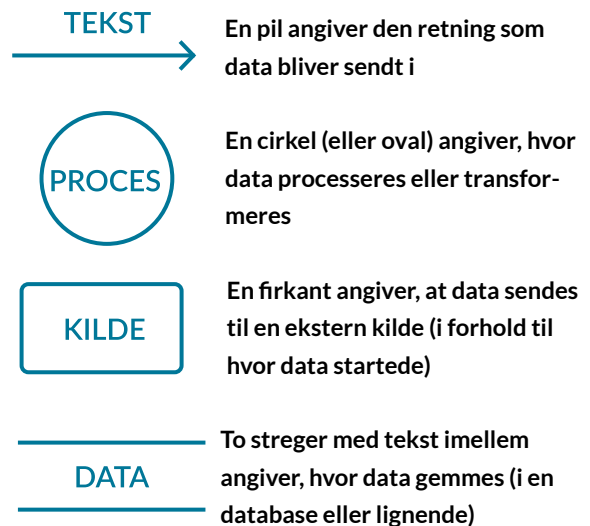
I skal være kreative i jeres formidling og tale målgruppens sprog. Så tag udgangspunkt i jer selv – hvad ville få jer til at stoppe op? Hvordan kommunikerer man på en måde, så målgruppen faktisk forstår, hvad data bliver brugt til? I har kun én side til jeres budskab, så det skal være enkelt og let at overskue.

I kan lave plakaten i hånden, på papir, i et tegneprogram, i PowerPoint eller noget tilsvarende.

2. DATAFLOW-DIAGRAM

Det kan være godt at spørge sig selv, hvad der sker med data, når de kommer til et system, om de omregnes eller konverteres på en eller anden måde eller gemmes i en database, og om hvordan data sendes videre til et nyt system eller et andet sted i systemet. Et dataflow-diagram viser, hvordan data strømmer igennem et system eller igennem en række af forskellige systemer. Det bruges ofte i softwareudvikling til at give et overblik over, hvor data er, hvornår og med hvilket formål.

Dataflow-diagrammet viser blandt andet, hvor data kommer fra, og hvor de går hen, hvor de bliver gemt og hvor de måske transformeres, eksempelvis fra stemme til skrift. **Følgende symboler kan bruges i diagrammet:**

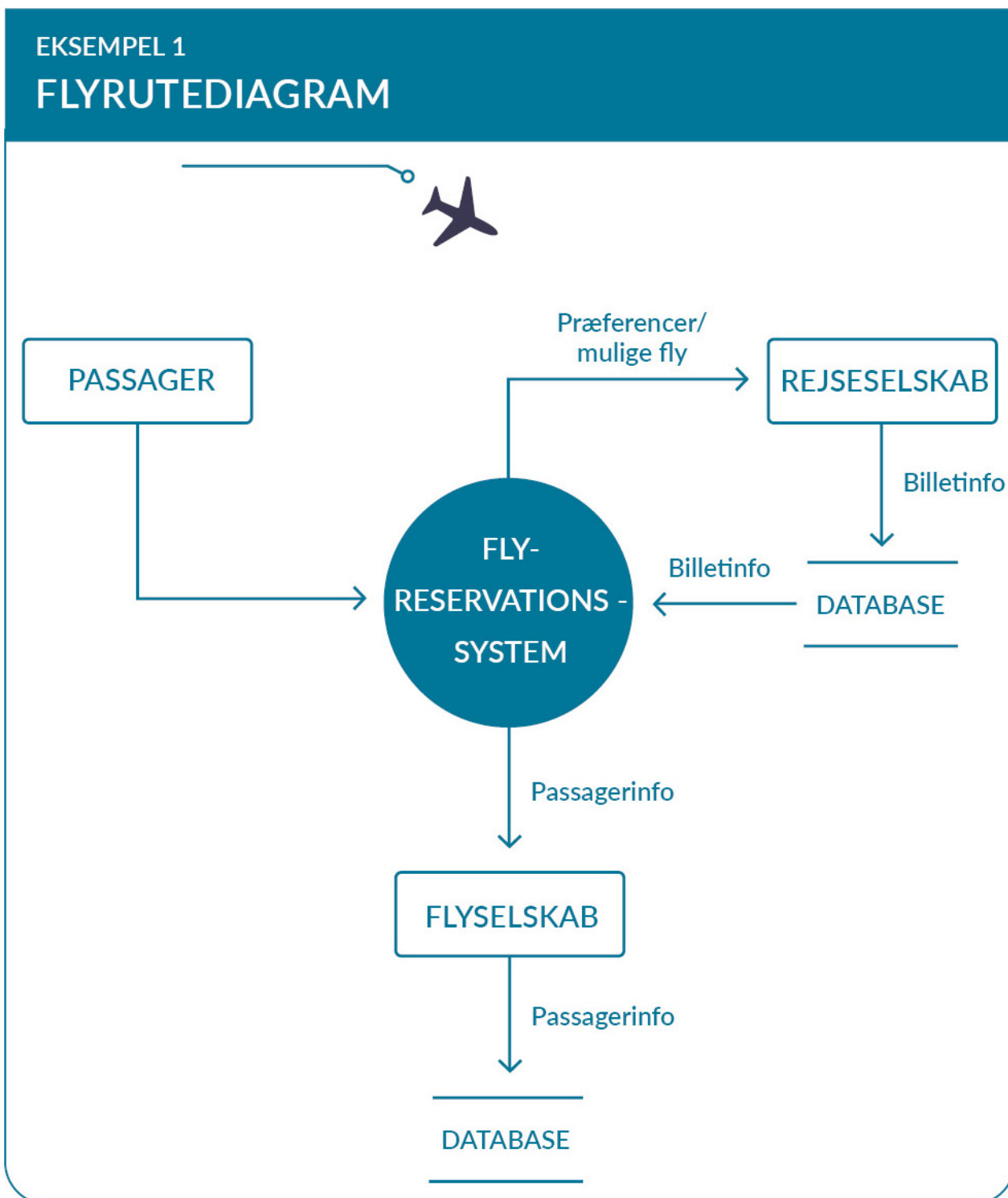


Man kan starte med et overordnet billede af, hvad der sker med data for at forstå nogle af de eksterne kilder. Derefter kan man dykke et skridt dybere for at forstå, hvad der sker på et detaljeret niveau.

Eksempel 1: Når man bestiller en flybillet:

Først søger man efter en rejse i et reserveringssystem. Systemet leder efter en bestemt rejse hos rejseselskabet, på baggrund af de kriterier man har indtastet, og finder en billet. Når billetten er fundet, sendes der en besked til flyselskabet, om at der er foretaget en reservation. Det kan se sådan ud i dataflow-diagrammet:

I eksemplet har vi ikke skrevet præcist hvilken data (navn, telefonnummer osv.), der overføres.



3. SÅDAN FINDER DU VIDEN OM COOKIES

Du kan finde informationer om cookies mange steder. Forbrugerrådet Tænk har udarbejdet en side, I eventuelt kan starte med at læse: <https://taenk.dk/test-og-forbrugertiliv/digitale-tjenester/privacy/cookies>.

Cookies har forskellige navne. Nogle navne er knyttet til den hjemmeside, man har brugt og indeholder typisk information om, hvordan du finder rundt på hjemmesiden og gemmer måske på login-information. Andre kan have navne, som gør det vanskeligt at forstå deres funktion.

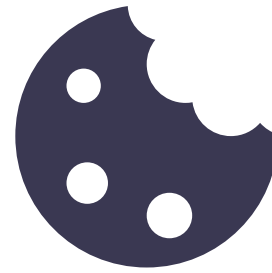
Prøv at finde ud af mere om cookies ved at google navnet på dem, I vil vide noget om. Det er ikke altid man kan finde noget information om dem, men ind i mellem kan man få information om, hvilken type de er. Ofte er den information på engelsk.

Slet cookies fra din browser

Det kan være vanskeligt at finde ud af, hvor cookies bliver gemt på en telefon eller en computer. Her er et par guides til, hvordan I tilgår og sletter data og cookies:

Ved anvendelse af safari på en iphone:

1. Gå til "indstillinger" og find "safari".
2. Gå derefter helt ned i bunden af siden til punktet "avanceret", så ser du "webstedsdata", som indeholder de cookies, din telefon har gemt.
3. Hvis I gerne vil fjerne alle cookies, er I stadig i fanen for "safari" – her kan I se en mulighed for at trykke på "fjern webstedsdata". Når I trykker her, vil alle jeres cookies blive slettet.



Ved anvendelse af FireFox på en android telefon:

1. Åben indstillingerne ved at trykke på de tre prikker i øverste højre hjørne, dernæst "indstillinger".
2. Scroll ned og tryk på "ryd private data"
3. Et nyt vindue åbner sig nu med forskellige muligheder. Vælg f.eks. "cookies & aktive logins". Hvis I dernæst trykker "Ryd data", fjernes alle jeres cookies.

Ved anvendelse af safari på en laptop:

1. Find "safari" og derefter "indstillinger".
2. Find herefter "sikkerhed og privathed", tryk derefter på "privathed" og find "håndter website data". Her finder du cookies og kan slette dem, du ikke vil have.

Ved anvendelse af Firefox på laptop:

1. Åben Firefox og gå derefter til "indstillinger".
2. Find herefter "privatliv og sikkerhed". Midt på den side finder du overskriften "cookies og websteds-data".
3. Tryk på "håndter data". Her kan du få et overblik over hvilke cookies, der er gemt. Du kan også bruge "ryd data" og på den måde fjerne alle cookies på en gang.

Andre browsere har tilsvarende områder, hvor du kan se cookies og fjerne dem.

JERES PRÆSENTATION

I skal forberede en præsentation af jeres løsning, hvor I redegør for jeres mission, fortæller om jeres proces med at finde frem til løsningsforslaget samt præsenterer selve løsningsforslaget.

I præsentationen skal I:

- Redegøre for jeres mission og den tematik, I har valgt at fokusere på
- Fortælle, hvordan I kom frem til jeres endelige løsningsforslag
- Præsentere jeres plakat og dataflow-diagram
- Fortælle, hvordan I formidler budskabet på jeres plakat, og hvordan I er kommet frem til datastrømmene i jeres diagram
- Argumentere for, hvilken effekt I tror, at jeres plakat kan få hos jeres målgruppe.

Præsentationen skal have karakter af et kort pitch, ligesom det de laver i Løvens Hule, og må max tage 10 minutter.

DELTA I EN NATIONAL KONKURRENCE

Cybermissionen er en national konkurrence, hvor alle ungdomsuddannelser har mulighed for at være med. Alle klasser må deltage i konkurrencen med ét løsningsforslag. Man deltager i konkurrencen ved at lave en videooptagelse af sin præsentation og sende den ind til Styrelsen for It og Læring. Alle videoer vurderes af et Cybermissionens dommerpanel.

Videoen skal uploades af den underviser, som har tilmeldt jer Cybermissionen. I finder link til uploadfunktionen på konkurrencens hjemmeside: <https://cybermissionen.cyberskills.dk/>, hvor I kan læse mere.



**”DANMARK ER EN
DIGITAL FRONTLØBER, OG
DET STILLER STORE KRAV
TIL BÅDE UNGE OG VOKSNE,
OM HVORDAN DE HÅND-
TERER OG BESKYTTER
DERES EGNE DATA.”**

BEGREBSLISTE

INCOGNITO / PRIVAT BROWSER



Når du sætter din browser i 'inkognito' gemmes dine indtastninger ikke i din browser eller lokalt på din computer. Men hjemmesider, din skole eller internetudbyder kan stadig se din aktivitet.

COOKIES



En cookie er en fil, der bliver gemt på din computer, når du besøger en hjemmeside. Nogle cookies er nødvendige for at hjemmesiden virker, andre husker hvad du klikker på, så hjemmesiden kan sende reklamer, som passer til dig. Når du besøger en hjemmeside, kan du vælge hvilke cookies du vil acceptere.

CYBER AWARENESS



Mange virksomheder laver cyber awareness træning. Det kan eksempelvis være kommunikationsaktiviteter eller uddannelse, der skaber opmærksomhed om informationsikkerhed hos medarbejderne, så de får en mere sikker digital adfærd.

DIGITALE FODSPOR



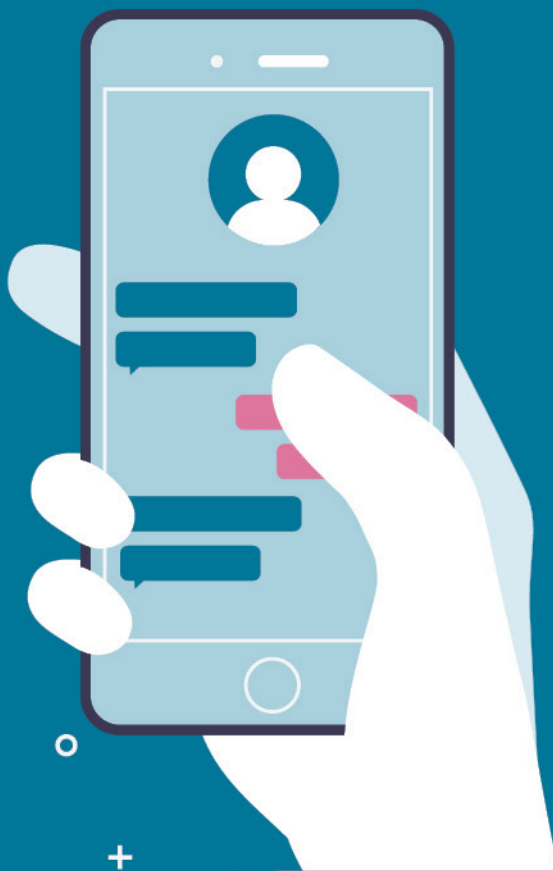
Når du søger på Google, sender en snap eller uploader en video på TikTok efterlader du dig spor på nettet, som bliver gemt. Det kaldes digitale fodspor, og de kan være meget svære at slette igen.

HACKING



Hacking er, når nogen ulovligt skaffer sig adgang til andres data - eksempelvis via en computer. Hackere udnytter svagheder i systemer. En svaghed kan eksempelvis være passwords, der er nemme at gætte.

Hvor mange begreber kender I?



GDPR



GDPR står for General Data Protection Regulation og er en lov, som er indført af EU for at passe på dine og alle andres data og personoplysninger.

TO-FAKTOR LOGIN



To-faktor login er en dobbelt lås, som typisk består af dit password og en kode, du får tilsendt - ofte på sms. Hvis andre får fat i dit brugernavn og password og forsøger at logge ind på din konto, kan det derfor ikke lade sig gøre, fordi de mangler den anden kode, som er sendt til din mobil.

MALWARE



Malware bruges om ondsindet software - fx virus eller andet, der skader din computer.

RISIKOANALYSE



En risikoanalyse er et værktøj, som har til formål at afdække potentielle risici ved at kategorisere dem ift. den mulige konsekvens og sandsynlighed for, at de indtræffer. Risikoanalysen anvendes dernæst til at prioritere ressourcer og beslutte hvilken handling, der skal sættes ind for at sikre, at det ikke går galt.

DDOS-ANGREB



DDos-angreb står for Distributed Denial of Service. Det er et digitalt angreb, hvor en hacker med vilje overbelaster en hjemmeside eller en it-service, så siden i en periode er utilgængelig eller bryder helt sammen. Angrebet udføres ved, at hackeren gennem et netværk af virusinficerede computere, et såkaldt botnet, sender en stor mængde forespørgsler til hjemmesiden og dermed får siden til at bryde sammen.

PHISHING



'Phishing' er, når it-kriminelle bruger falske e-mails, links eller hjemmesider til at få fat i andres private oplysninger, eksempelvis til banken. Det er tit svært at se forskel på, hvad der er falske links, mails og hjemmesider, og hvad der er ægte.

Kan I finde flere ord?