VELKOMMEN TIL

CYBERMISSIONEN

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

CYBER SKILLS

Velkommen til Cybermissionen

ISBN nr:
87-603-3299-9 (web udgave)
87-603-3300-6 (trykt udgave)

Design:
Børne- og
Undervisningsministeriet

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

INDHOLDSFORTEGNELSE

I dette materiale, vil der være links og henvisninger til digitale ressourcer og videomateriale, som er tilknyttet Cybermissionen. I det digitale materiale, som ligger på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/ vil alle henvisninger og videoer være klikbare og lette for dig og dine elever at finde.

CYBERMISSION 1 - CYBER AWARENESS

Mange unge oplever, at de har godt styr på deres adfærd på nettet, at de ved, hvad de skal sige ja og nej til, hvad de skal undgå at klikke på og hvad de generelt skal undgå af fælder - måske tænker du det samme?

Men flere undersøgelser viser, at mange ikke altid gør det, de godt ved, de burde gøre i forhold til datasikkerhed.

Det er faktisk ikke kun unge, der mangler viden om datasikkerhed og har brug for en bedre digital adfærd. Det er også et af de områder, som er i fokus hos danske virksomheder: At styrke medarbejdernes viden om, hvordan man agerer sikkert på nettet.

Den udfordring skal I hjælpe med at løse!

IT-SIKKERHED ER MEGA COOL!

De it-løsninger, vi bruger til dagligt, skal helst bare virke, gerne hurtigt, allerhelst uden bøvl og alt for mange krav når man skal oprette konti, logge ind osv. Men sikkerhed betyder også, at det nogle gange bliver besværligt.

For mange er det svært at forstå, hvor stor faren er på nettet, når vi bruger digitale løsninger. Vi kan nemlig ikke altid se de konsekvenser, "små handlinger" kan lede til.

It-sikkerhed er et vigtigt område, der skal mere fokus på, og det er det, I skal arbejde med på denne mission. På denne mission bliver I mestre i god digital adfærd, og så skal I overbevise andre om, at de også skal være opmærksomme på deres it-sikkerhed!

JERES MISSION

I jeres gruppe skal I udvikle en kommunikationskampagne, der henvender sig til målgruppen unge i alderen 15-25 år. I må gerne snævre målgruppen endnu mere ind.

I det følgende finder I tre aktuelle temaer, som kan være omdrejningspunktet for jeres kommunikationskampagne. I kan bruge én eller flere eller selv komme på en tematik. Det vigtigste er, at kommunikationskampagnen kan forbedre målgruppens digitale adfærd - med fokus på it-sikkerhed. Når I har lavet en kampagne, skal I også forberede en kort præsentation, hvor I fortæller om tankerne bag.

TEMA 1

STYRK DIT PASSWORD

I skal få målgruppen til at lave bedre passwords og passe godt på dem.
De fleste laver forudsigelige passwords, der er lette at gætte/hacke, bruger det samme password til facebook og e-mail m.m. og deler det også med andre, når de eksempelvis låner deres Netflix-konto ud.

TEMA 2

HUSK AT LÅSE DIN COMPUTER

I skal få målgruppen til altid at låse deres computer, når de forlader den.
Hvor tit har I ikke forladt jeres plads uden at låse jeres computer? Det sker alt for tit, og I skal derfor gøre målgruppen opmærksom på, at de skal låse deres computer, så andre ikke får adgang til information, der ikke vedkommer dem.

TEMA 3

UNGÅ AT BIDE PÅ "PHISHING-KROGEN"

I skal lære målgruppen ikke at klikke på links i mails, som de ikke har tillid til.
En phishingmail er, hvor en hacker forsøger at franarre (fiske) éns personlige oplysninger som eksempelvis passwords. De prøver at lokke en til at klikke på et link i en mail, hvorefter de kan se de oplysninger, man indtaster. I skal derfor lære målgruppen at genkende phishingsmails, så de ikke ryger på krogen.

KAMPAGNENS FORMAT

I bestemmer selv, hvordan kommunikationskampagnen skal udformes. Den kan se ud på mange måder og I kan finde inspiration i listen her:

- SoMe-kampagne
- Informationsmail
- Film (el. et storyboard til en film)
- Podcast
- Et event (lav evt. en drejebog for et event)
- Quiz
- Plakat
- Pjecer

Overvej hvordan I kan lave budskabet sjovt, anderledes, kreativt og/eller nytænkende. Det er vigtigt, at kampagnen får målgruppen til at stoppe op en ekstra gang - og rent faktisk ændrer deres digitale adfærd. I kan med fordel tænke på situationer og scenarier, som målgruppen let kan relatere til.

Der forventes ikke et helt færdigudviklet produkt. Hvis I synes, I kommer bedst igennem med jeres budskab ved at lave et event, skal I ikke afholde et event, men I kan eksempelvis lave en drejebog for et event med et program, indholdspunkter mm.

GODE RÅD TIL KAMPAGNEUDFORMING

Når I skal i gang med at lave selve kampagnen, er det en god ide at starte med at finde ud af, hvilket budskab I vil kommunikere, hvilken adfærd I ønsker at ændre og hvem I kommunikerer til. Her kan I med fordel undersøge lidt mere om emnerne og måske også få inspiration fra andre.

Derudover kan I få hjælp i diverse kommunikationsmodeller. Hvis ikke I allerede har arbejdet med nogen i undervisningen, kan I bruge de to modeller, som er beskrevet i det følgende. Det er "Argumentationsanalysen" og "Kommunikationsmodellen".

Modellerne kan hjælpe jer i de valg, I træffer, når I udformer jeres kommunikationskampagne.

"OFTEST ER DET HELT BASALE MENNESKELIGE FEJL, DER GØR AT EN VIRKSOMHED UDSÆTTES FOR DATABRUD."

MODEL 1: ARGUMENTATIONSANALYSEN

I argumentationsanalyse skelner man mellem tre appelformer, der beskriver, hvordan man taler til modtageren på tre forskellige måder: Logos, etos og patos

Når man arbejder med budskaber, er det en god ide at overveje sin appelform.

I jeres præsentation skal I redegøre og argumentere for, hvordan I bruger de forskellige appelformer i jeres kommunikation. I kan sagtens anvende flere appelformer.

ETOS

Etos som appelform handler om at skabe troværdighed omkring afsenderen på baggrund af en person og hans eller hendes værdier. Hvis modtageren har tillid til afsenderen, er man oftest mere tilbøjelig til at give afsenderen ret i vedkommendes synspunkter og budskaber.

LOGOS

Denne appelform handler om at overbevise modtageren via en saglig og rationel argumentation. Man taler til modtagerens fornuft for at få dem til at indse rigtigheden af afsenderens synspunkter eller teorier. Logos bygger på fakta, tekstbelæg, statistikker og tal, altså dét som kan måles og dokumenteres.

PATOS

Denne appelform henvender sig til modtagerens følelser. Når afsenderen benytter patos som appelform, forsøger man at vække følelser som glæde, ophidselse, frygt, medlidenhed eller vrede hos modtageren for på den måde at overbevise ham eller hende om sit synspunkt.

MODEL 1

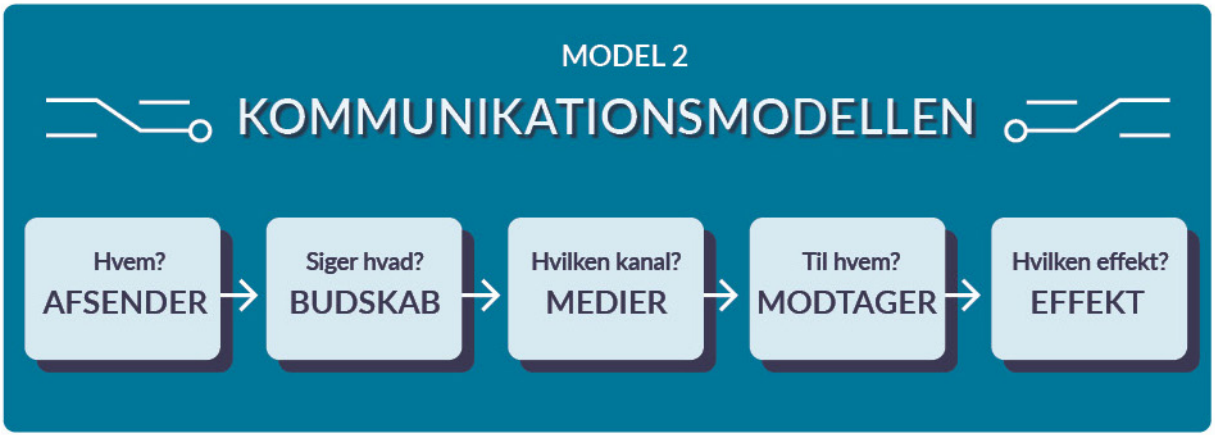
ETOS, LOGOS OG PATOS

TYPE	ETOS	LOGOS	PATOS
BETYDER	Når han/hun gør det, må det være godt	Tal, data, videnskabelige beviser Det logiske, det der tilsyneladende ikke kan sættes spørgsmålstegn ved	Gør det for min skyld Følelsestale
EKSEMPEL	"Fordi jeg siger det ..."	"Hvis du gør sådan sker der det og det ..." "70% af den danske befolkning ville gøre sådan..."	"Jeg bliver skuffet hvis du ikke gør det ..."

MODEL 2: KOMMUNIKATIONSMODELLEN

Kommunikationsmodellen, som I kan se herunder, består af fem faser, og kan hjælpe én, når man skal overveje sit budskab, udformning af budskabet, hvordan man vælger at kommunikere det samt om man via sine valg opnår den ønskede effekt.

I kan bruge kommunikationsmodellen til at beskrive jeres kampagne. I må gerne erstatte modellen med andre modeller, som I har kendskab til, og som I måske synes er bedre.



AFSENDER - Hvem?

"Hvem er det som siger noget?"
Afsender er den, der vil kommunikere et givent budskab.

BUDSKAB - Siger hvad?

"Hvad bliver der sagt?"
Afsenderens budskab er det, som han eller hun ønsker at kommunikere til modtageren.

MEDIE - I hvilken kanal?

"Hvordan og hvor bliver det sagt?"
Medie er den kanal, der bruges til at formidle budskabet (det kan være alt fra en fysisk plakat, et nyhedsbrev, en kampagne på sociale medier osv.).

MODTAGER - Til hvem?

"Hvem bliver det sagt til?"
Modtageren er den person, afsenderen vil sende sit budskab til.

EFFEKT - Med hvilken effekt?

"Hvad hører modtageren der bliver sagt?"
Modtagerens afkodning af budskabet og en analyse af, hvordan modtager bliver påvirket af afsenderens meninger/budskab.

INSPIRATION

Inden I går i gang med at lave kommunikationskampagnen, kan I starte med at se disse tre videoer, som er lavet sammen med nogle super dygtige folk, der arbejder med kommunikation og it-sikkerhed til daglig. De vil hjælpe jer til at forstå missionen, og I får nogle gode tips til stærke budskaber. Videoerne varer mellem 8-12 minutter:

Video 1)
Cybersecurity Awareness - Hvem beskytter vi os mod?

Video 2)
Tips og tricks til gode cyber awareness kampagner

Video 3)
Når budskaber skal fange

JERES PRÆSENTATION

I skal forberede en præsentation af jeres kommunikationskampagne, hvor I redegør for missionen, fortæller om jeres proces med at finde frem til jeres løsning 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 kommunikationskampagne (gerne med billeder, video m.m)
- Fortælle, hvordan I har anvendt analyseredskaber ex. argumentationsanalysen eller kommunikationsmodellen
- Argumentere for, hvilken effekt I tror, at jeres kampagne 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.

DELTAG 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 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.

CYBERMISSION 2 - TRUSSELSVURDERING OG RISIKOANLYSE

Danmarks sikkerhed er vigtig for os alle, ung som gammel. Men hvordan beskytter vi bedst Danmark mod de mange kriminelle, der findes ude i cyberspace? Og hvad er egentlig vigtigst for os at beskytte i Danmark?

Danmark har udarbejdet en national strategi for cyber- og informationssikkerhed (læs den her: https://digst.dk/strategier/cyber-og-informationssikkerhed/). Strategien afspejler et ønske om at opruste den samlede indsats i kampen mod de digitale trusler, Danmark står overfor. I strategien er der udpeget seks samfundskritiske sektorer, som det kræver en særlig indsats at beskytte mod trusler.

De seks samfundskritiske sektorer er valgt, fordi det vil være meget kritisk, hvis en virksomhed inden for en af disse sektorer blev offer for et hackerangreb.
De seks udvalgte sektorer er: tele-, finans-, energi-, sundheds-, transport- og søfartssektoren. Det omfatter eksempelvis teleselskaber, banker, elselskaber, sygehuse, offentlig transport som DSB og de, som opererer på havet.

SEKTORANSVARSPRINCIPPET

I Danmark er det bestemt, at sektorerne bærer et "sektoransvarsprincip". Det betyder, at den enkelte sektor har ansvar for at sikre et vist beredskab, så de kritiske funktioner kan opretholdes. Det betyder, at virksomhederne skal tage et aktivt ansvar for at være beredt på cyberangreb.

I energisektoren har man eksempelvis stiftet foreningen EnergiCERT (Link: https://energicert.dk/). EnergiCERT har til formål at løfte sektorens cyber- og informationssikkerhedsniveau og støtte sektoren i at agere professionelt mod cybertrusler.

Ansvaret for cybersikkerhed er altså ikke samlet et enkelt sted, men det er placeret i alle sektorer. I Danmark ser man cybertruslen som en samfundsudfordring, der skal løses i fællesskab mellem stat, kommuner, regioner, organisationer, virksomheder og os alle som privatpersoner. Alle har et ansvar.

RISICI VED HACKERANGREB

Man tænker måske ikke over det til hverdag, men det vil være ret alvorligt, hvis den danske telesektor blev lagt ned af et hackerangreb. Det kan få den betydning, at vores telefoner ikke længere kan få adgang til data, og der kan potentielt set blive lukket ned for al kommunikation i landet.

Et succesfuldt cyberangreb mod telesektoren kan medføre økonomiske tab for virksomheder, afsløre fortrolige data og påvirke tilgængeligheden af teletjenester. De angreb, som eksempelvis bliver brugt mod telesektoren, er det, man kalder DDOS-angreb (overbelastningsangreb), ransomware, der rammer kritiske systemer, eller uautoriseret omdirigering af mobil- og internettrafik.
Læs mere om de forskellige typer angreb her: https://sikkerdigital.dk/virksomhed/hvad-truer-din-virksomhed

Center for Cybersikkerhed vurderer, at telesektoren i Danmark står over for en **MEGET HØJ** trussel fra cyberkriminalitet. Så cybertrusler er altså en realitet for telesektoren og noget, de skal forholde sig til hver eneste dag.

RISIKOANALYSER OG TRUSSELSVURDERINGER

Prøv at forestille dig, at du blev nægtet adgang til al mobiltelefoni og internetadgang? Det er ikke kun privat, at folk vil opleve det som en katastrofe, for mobiltelefoni og internetadgang er afgørende for alle dele i samfundet.

Teleselskaber har altså et stort ansvar for at beskytte sine it-systemer og undgå sikkerhedsbrud. De laver løbende trusselsvurderinger, risikoanalyser og analyserer sårbarheder for at forhindre det næste potentielle angreb. De er meget opmærksomme på hvilke typer

angreb, der dominerer sektoren, så de kan forberede sig bedst muligt.

JERES MISSION

På denne cybermission skal I forestille jer, at I er blevet hyret ind af ledelsen i en af Danmarks største televirksomheder. I skal hjælpe dem med at undersøge hvilke forhold og risici, de skal være opmærksomme på i deres omverden, når det kommer til it-sikkerhed. Derudover skal I lave en vurdering af de konsekvenser, der er forbundet med de forskellige risici. Med andre ord skal I lave det, man kalder en trusselsvurdering.

Med grundig forberedelse kan man som firma nemlig styrke sit forsvar og være bedre forberedt på angreb.

I får stillet to værktøjer til rådighed, som danner grundlaget for jeres trusselsvurdering: **1) Omverdensanalyse** og **2**) **Risikoanalyse**, som begge beskrives nedenfor.
Når I har lavet de to analyser, skal I forberede en præsentation til ledelsen, hvor I skal fremlægge det I har fundet ud af og hvilke handlemuligheder virksomheden har.

MODEL 1) OMVERDENSANALYSE

En virksomhed er nødt til at analysere sin omverden for at kunne se, hvad der kan påvirke dens situation og udvikling. Omverdensanalysen er et godt værktøj til at afdække alt fra politiske faktorer til teknologiske forhold, der spiller en rolle og påvirker situationen for virksomheden.
Når man laver en omverdensanalyse kigger man på virksomhedens "afhængige omverden" og den "uafhængige omverden", som illustreret i model 1.
Den afhængige omverden, også kaldet "nærmiljøet", er de forhold, som virksomheden har påvirkning på og direkte kontakt med. Den uafhængige omverden, også kaldet "fjernmiljøet", er de overordnede forhold, som påvirker virksomheden. Selvom virksomheden ikke har direkte indflydelse på den uafhængige omverden, er det vigtigt, at den holder sig orienteret om, hvad der sker.

Jeres opgave er altså at tage plads i sædet som rådgiver for televirksomheden, og analysere dens omverden i forhold til cybertrusler, it-kriminalitet og mulige angreb. I skal se på både den afhængige og den uafhængige omverden.

Følgende spørgsmål kan hjælpe jer på vej med analysen. Spørgsmålene tager afsæt i **Omverdensmodellen**.

Spørgsmål til den afhængige omverden:

- **Kunderne:** Hvordan vil kunderne reagere, hvis virksomheden bliver offer for et cyberangreb
- **Konkurrenter:** Hvordan vil det påvirke konkurrenternes position, hvis virksomheden bliver offer for et cyberangreb?
- **Leverandører:** Hvordan vil det påvirke virksomheden, hvis en af deres leverandører bliver offer for et cyberangreb?

Spørgsmål til den uafhængige omverden:

- **Politik og lovgivningsmæssige forhold:** Hvordan kan politiske, bl.a. internationale forhold, motivere cyberangreb?

- **Politik og lovgivningsmæssige forhold:** Hvordan kan ny lovgivning påvirke måden, hvorpå virksomheden arbejder med informationssikkerhed?
- **Teknologiske forhold:** Hvilke teknologiske forhold skal virksomheden være opmærksom på for fortsat at beskytte sig selv og sine kunder mod cyberangreb?
- **Teknologiske forhold:** Hvordan kan den øgede digitalisering af samfundet have indflydelse på risikoen for, at virksomheden bliver offer for et cyberangreb?
- **Massemedier:** Hvad er massemediernes rolle, når det gælder hackernes motivation for at lave angreb?

MODEL 2)
RISIKOANALYSE

Risikoanalysen bliver ofte anvendt af virksomheder. Man bruger den til løbende at holde styr på hvilke risici, der er de mest alvorlige og til at finde strategier til at reducere, udbedre og overkomme disse risici.
Der vil altid være en lang liste af forskellige risici, men det er langt fra alle, der er lige sandsynlige eller har samme konsekvenser.

En risiko består altid af

1. **En sandsynlighed for hændelsen**
2. **Konsekvenser af hændelsen**

Det er ikke et mål i sig selv at undgå risici, men målet er at sikre, at risici håndteres, eller at man vurderer, at den ikke skal håndteres lige nu, da den ikke er vigtig. Her kan man bruge risikoanalysen til at sikre den rigtige prioritering.

I skal identificere minimum fem risici som televirksomheden står overfor. Nogle tager måske udgangspunkt i jeres drøftelser i forbindelse med jeres omverdensanalyse, andre er måske helt nye.
I må bruge jeres fantasi og finde på 'ekstreme tilfælde" og også gerne nogle som er mere almindelige og dermed mere sandsynlige. En risiko kan være alt fra indførelse af ny lovgivning til risikoen for, at der opstår en "hacker-aktivist-gruppe", der er imod virksomhedens forretningsområde.

Et eksempel på en risici:

"Organiseret netværk af cyberkriminelle fra Kina lægger hele Danmarks mobilnet ned – man mener at angrebet er politisk motiveret."

I skal huske at argumentere for, hvorfor I har indplaceret den pågældende risici I det givne felt.

MODEL 2

RISIKOANALYSE

KONSEKVENSER

SANDSYNLIGHED

	1 Ubetydelige	2 Mindre	3 Alvorlige	4 Meget alvorlige	5 Katastrofale
5 Ofte	5	10	15	20	25
4 Sandsynlig	4	8	12	16	20
3 Sjælden	3	6	9	12	15
2 Usandsynlig	2	4	6	8	10
1 Meget usandsynligt	1	2	3	4	5

INSPIRATION

Inden I går i gang anbefaler vi, at I ser følgende videoer, hvor I møder en række super dygtige folk, som arbejder med området til daglig. De vil hjælpe jer med at forstå missionen, modellerne og give jer gode tips. Videoerne varer mellem 8-12 minutter.

VIDEO 1)
Hvordan beskytter vi Danmarks kritiske infrastruktur?

VIDEO 2)
Hvad påvirker trusselsbilledet i Danmark?

VIDEO 3)
Hvad er en risikoanalyse?

VIDEO 4)
Sådan laver man en omverdensanalyse

"NÅR CYBERKRIMINELLE GÅR EFTER KRITISK INFRASTRUKTUR SOM FX HOSPITALER, FORSYNINGSSELSKABER OG TELENETVÆRK, KAN DET BRINGE BÅDE SIKKERHED OG SUNDHED I FARE."

JERES PRÆSENTATION

I skal forberede en præsentation til ledelsen i virksomheden, hvor I fremlægger jeres analyser, gerne med brug af visuelle virkemidler

I præsentationen skal I:

- Præsentere de forhold I har fundet frem til i jeres omverdensanalyse
- Fremlægge de risici I har udvalgt til jeres risikoanalyse, vise hvordan I har indplaceret dem i jeres risikoanalyse (sandsynlighed/konsekvenser) og forklare hvorfor
- Fortæl kort, hvorfor det er vigtigt, at virksomheder forholder sig til deres omverden når det kommer it-sikkerhed og cyberangreb.

I må meget gerne underbygge jeres præsentation med aktuel viden og kilder.

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

DELTAG 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 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.

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 cyberkriminel kan bryde ind i vores mailboks eller på anden vis få adgang til ens personlige oplysninger.

IT-SIKKERHED ER IKKE ALTID LIGE SJOVT!

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.

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:**

En pil angiver den retning som data bliver sendt i

En cirkel (eller oval) angiver, hvor data processeres eller transformeres

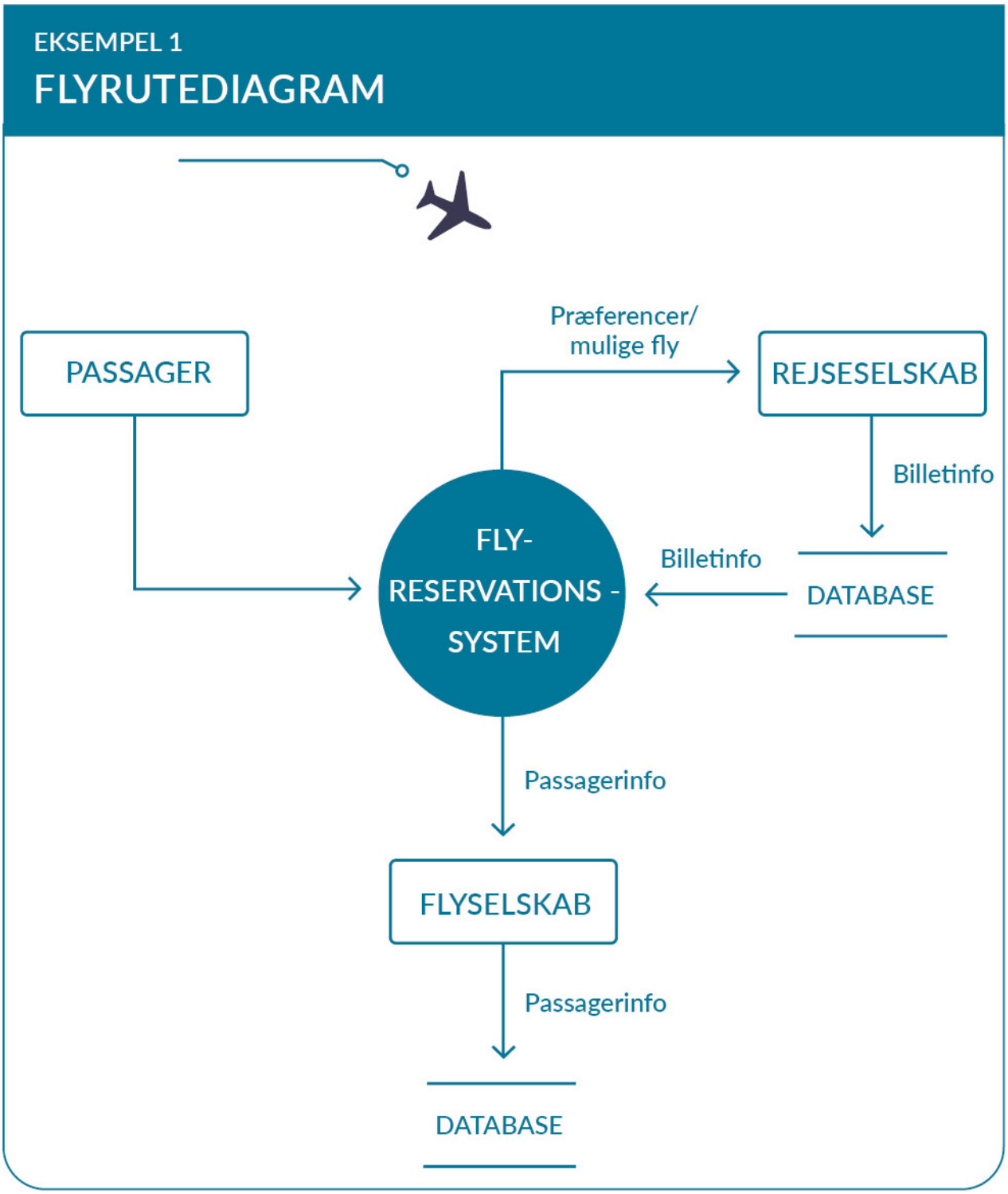
En firkant angiver, at data sendes til en ekstern kilde (i forhold til hvor data startede)

To streger med tekst imellem angiver, hvor data gemmes (i en database eller lignende)

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.

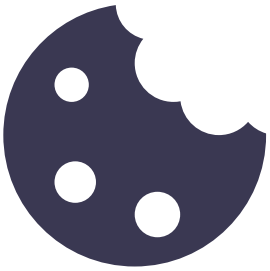
Eksempel 1: Når man bestiller en flybillet:
Først søger man efter en rejse i et reserveringssystem. Systemet leder efter en bestemt rejse hos rejseselskabet, på baggrund af de kriterier man har indtastet, og finder en billet. Når billetten er fundet, sendes der en besked til flyselskabet, om at der er 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-forbrugerliv/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.

DELTAG I EN NATIONAL KONKURRENCE

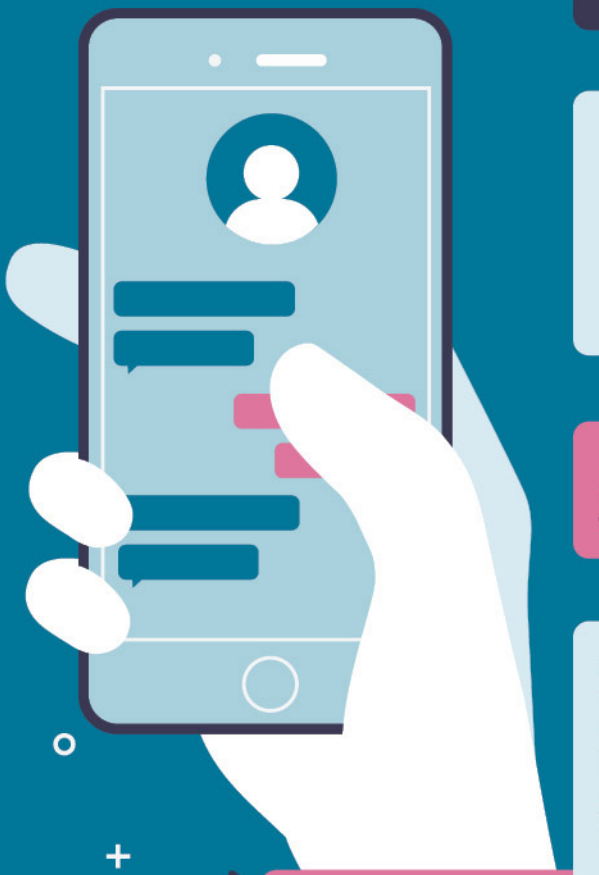
Cybermissionen er en national konkurrence, hvor alle ungdomsuddannelser har mulighed for at være med. Alle klasser må deltage i konkurrencen med ét løsningsforslag. Man deltager i konkurrencen ved at lave en videooptagelse af sin præsentation og sende den ind til Styrelsen for It og Læring. Alle videoer 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 HÅNDTERER OG BESKYTTER DERES EGNE DATA."

CYBERMISSIONEN

BEGREBSLISTE

Hvor mange begreber kender I?



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 informationssikkerhed 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.

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.

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.

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?

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR IT OG LÆRING
CYBER SKILLS

CYBERMISSIONEN - NOTER

CYBERMISSIONEN - NOTER

CYBERMISSIONEN

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR IT OG LÆRING

CYBER SKILLS