# CYBERMISSIONEN

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

CYBER SKILLS

# MISSION 2: PRIVACY OG CYBERMOBNING

Har du nogensinde følt, at ting er gået helt amok på nettet og du ikke havde kontrol over dine personlige oplysninger? Denne mission handler om at kontrollere og sikre dine informationer og dit privatliv online.

## DINE DATA PÅ NETTET

Vi bruger vores personlige data hver dag, for eksempel på hospitaler, i skolen og når vi er i kontakt med forskellige virksomheder. Vi deler også informationer om vores liv, fritid og færden på spilsider, sociale medier og apps. Det er med andre ord umuligt at gå gennem hverdagen uden, at der bliver opsamlet data om en.

Vores aktiviteter online overvåges, gemmes og analyseres af både firmaer og offentlige myndigheder. Gennem den data de opsamler får de viden om deres brugeres adfærd og behov, så de kan udvikle og forbedre de services de sælger eller stiller til rådighed.
Der er altså en række gode grunde til at dataopsamlingen sker, men det medfører også den risiko, at dataen kan blive misbrugt. Som denne mission afslører, er det ikke kun virksomheder, der kan bruge den data, der er tilgængelige om os på nettet – den kan også bruges af private personer.
Det er derfor vigtigt at skabe en bevidsthed om privatliv blandt alle, også unge mennesker. Denne mission skal få jer til at tænke over, hvordan I kan beskytte jeres private data, hvordan I kan surfe på internettet uden at efterlade jer spor, og hvordan I kan forblive anonyme på internettet. I skal som del af missionen lære om "cyberhygiejne" det vil sige, hvordan du beskytter dit privatliv online. Men det kræver, at I selv bruger jeres research-evner til at finde svarene.

Inden I går i gang med missionen kan I se en introvideo om trolling og digital chikane. I finder videoen under videomateriale på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/

## JERES MISSION

Mission 2 fokuserer på personer, der forfølger andre personer online. I skal arbejde med og reflektere over vigtigheden af at være forsigtig på nettet, overveje etikken og den potentielle skade, cybermobning kan gøre.

Vigtigst af alt sætter missionen fokus på, hvorfor gode vaner for cybersikkerhed og privatliv online er vigtigt. Vi håber at missionen kan inspirere jer til gode overvejelser og give jer ny viden om god cyberhygiejne.

Missionen er inddelt i tre sektioner. Der er spørgsmål undervejs som I skal tænke over og tale om for at kunne besvare dem. Til sidst skal I opsummere det hele i et kommunikationsprodukt, eksempelvis en plakat.

## TEENAGER BLIVER OFFER FOR TROLL-ANGREB

I vil få præsenteret en case, der gennemgår historien om en teenager, der bliver mål for cybermobning efter, at hendes post på Instagram går viralt.

Casen begynder med, at mobningen kun sker på de sociale medier. Men det eskalerer gradvist til at påvirke offeret og hendes familie også i den fysiske verden.

Situationen kommer mere ud af kontrol, da mobberne får adgang til hendes konti, og hun bliver offer for cyberkriminalitet.

Denne case er fiktion, men den er lavet ved at kombinere elementer fra flere virkelige historier. Så det kunne faktisk have været dig, din ven eller din nabo.

# CASEN

## ANNAS OPSLAG PÅ INSTAGRAM RESULTERER I TROLL-ANGREB

Anna er en typisk gymnasieelev i Danmark. Hun har et godt socialt liv og er aktiv på flere sociale medier.

Annas 500 Instagram-følgere er mest hendes venner, folk fra samme skole og hendes familie. Hendes konto er ikke privat, men nærmest ingen udenfor hendes sociale cirkel liker eller deler det, hun poster.

## DEL 1

## EN POST GÅR VIRALT PÅ SOCIALE MEDIER, OG MOBNINGEN BEGYNDER

En dag poster Anna et foto på Instagram med en joke om et populært fodboldhold, der lige har tabt til hold, der normalt ikke klarer sig særligt godt – hun knytter et par hashtags til billedet. Hun tænker ikke så meget over indholdet og har faktisk ikke engang stærke følelser omkring det. Men hun deler det, fordi hun synes, at det er sjovt.

Flere dage senere går en populær influencer, som Anna hverken kender eller følger, gennem posts med et af de hashtags som Anna brugte til sit opslag. Influenceren ser fotoet med joken og bliver irriteret over det. Influenceren deler et screenshot og Annas profilnavn på Instagram. Nu kan over 100.000 mennesker se Annas post, hvilket er 200 gange flere end dem, der normalt ser hvad Anna poster på Instagram – og dermed også mange mennesker, som Anna slet ikke havde tænkt skulle se joken.

Næste morgen vågner Anna op til tusindvis af notifikationer på sin mobil. Hendes profil får pludselig besøg af tusindvis af mennesker – såkaldte trolls/trolde - der kommenterer på hendes nuværende og gamle posts. Mange deler influencerens screenshot med kommenterer med alt fra fornærmelser som ”dumme tøs” til trusler om at ”hun burde skydes”.

Anna skynder sig at slette det oprindelige foto, men folk holder ikke op med at kommentere, og de går videre til hendes ældre posts. Anna ender med at gøre sin profil privat og ændrer kontonavnet for at stoppe dem.

Men raseriet stopper ikke der. Der er stadigvæk trolls, der sender Annas posts i omløb, deler screenshots af hendes posts med kommentarerne og laver nye hashtags om at “cancel” hende. Det lykkedes også for dem, der chikanerer Anna, at identificere hendes kæreste og flere nære venner ud fra Annas billeder, hvilket betyder at de nu også bliver chikaneret af ”troldene”.

## ARBEJDSSPØRGSMÅL

## HVORDAN AFVÆRGER MAN BEDST ET TROLL-ANGREB?

Arbejdsspørgsmål til del 1:

1. Lav en liste over de ting, der førte til troll-angrebet mod Anna, hendes kæreste og venner.
2. Sortér listen mellem de ting, som Anna selv har kontrol over og de ting, der er udenfor hendes kontrol.
3. Hvad kunne Anna have gjort anderledes for at undgå troll-angrebet?
4. Hvad skal Anna gøre nu, hvor chikanen fortsætter?
5. Hvor går grænsen for jokes?
   Det kan være svært, at forstå, hvorfor så mange folk begynder at chikanere Anna. Men det, som virker som en sjov og ufarlig joke for en person, kan virke voldsomt og helt urimeligt på en anden person. Prøv at lave nogle eksempler på jokes om for eksempel et fodboldhold, og diskuter hvilke I selv ville have lyst til at dele på sociale medier – og hvilke I tænker er over grænsen. Ser I forskelligt på det? Og er der forskelle på, hvad I vil dele hvor og med hvem?

**TIP: Tænk på, hvorvidt internettet er et frit miljø, hvor alle skal have lov til at dele deres meninger - og om I synes, at folk har ret til at svare Anna? Hvor går grænsen mellem at udtrykke sig og at chikanere? Og hvor går grænsen mellem, hvad der en sjov joke og hvad der er mobning?**

## DEL 2

### CHIKANEN NÅR DEN VIRKELIGE VERDEN

Ukendte personer fra internettet får opsporet Annas fulde navn, og ved at google og **søge forskellige steder**, finder de frem til Annas telefonnummer, e-mailadresse, og hvor hun bor. Annas kontaktoplysninger bliver delt i et anonymt online-forum, og de spredes mellem de mennesker, der var rasende over hendes oprindelige post om fodboldholdet.

Det betyder, at Anna begynder at blive ringet op af folk, hun ikke kender, hvilket hun heldigvis kan stoppe ved at få nyt telefonnummer. Men hun oplever også chikane i form af, at få leveret pizza, hun ikke har bestilt - og der bliver kastet skrald på hendes vinduer. Mest alvorligt er, at hun får flere dødstrusler sendt med posten.

Tingene når kogepunktet, da en person ringer til Annas far og udgiver sig for at være fra politiet. Annas far opdager hurtigt, at det ikke er en rigtig politibetjent og råber af personen i ren frustration. Hans reaktion bliver optaget og bagefter bliver Annas fars svar, som er fyldt med bandeord, lagt på internetsiden 4chan. Troldene glæder sig over mandens vrede, og Annas far bliver brugt som internetmemes.

Nu får hele familien nye hemmelige telefonnumre.

### ARBEJDSSPØRGSMÅL

1. Hvordan tror I, at troldene kunne de finde Annas privatadresse?
   - *Lav en liste over alle de steder og spor, der kan bruges til at finde frem til hvor en person bor.*

**TIP: Husk, at alt, hvad vi gør online, efterlader et spor. Posts, der ser uskyldige ud, kan bruges til at identificere privat information.**

2. Hvad kunne Anna have gjort for at begrænse udbredelsen af hendes personlige oplysninger?

**TIP: Undersøg hvad nøglebegreber som doxing og oversharing betyder.**

***"1 UD AF 7 DANSKERE MELLEM 18 OG 34 HAR OPLEVET AT BLIVE CHIKANERET ELLER STALKET PÅ NETTET"***

***(Userneeds, ingeniørforeningen IDA, 2017)***

3. Hvad skal Anna gøre nu, hvor fremmede truer hende og hendes familie?

**TIP: Undersøg hvem, der kan hjælpe familier i samme situation som Annas (myndigheder og andre) og hvad de anbefaler at man gør.**

## DEL 3

### UAUTORISERET ADGANG

Anna har ikke været særlig opmærksom på sikkerhed online, og har brugt den samme, meget simple, adgangskode til alle sine konti. Et af de steder, hvor Anna har brugt sin adgangskode, er et online forum – der i en helt anden situation, som ikke har noget med troll-angrebet på Anna at gøre, har været offer for hacking. Hackerne delte kontonavne, e-mailadresser og adgangskoder for tusindvis af mennesker i flere fora, og nu er Annas kontoinformationer pludselig interessante for troldene at finde. På grund af hacket og det, at hun brugte den samme adgangskode overalt, kan enhver finde både hendes e-mailadresse og adgangskode med en googlesøgning.

Troll-angrebet bliver udvidet, da angriberne finder og bruge den samme adgangskode til at få adgang til Annas e-mailkonto. Ved at se på kontoens e-mailhistorik kan angriberne også se, hvilke sider og apps hun er registreret på. Anna har blandt andet en Snapchatkonto, som angriberne nu kan bede om at få et nyt kodeord til, fordi de kender hendes e-mailadresse. Efter de får den nye kode, har angriberne fri adgang til kontoen, og kan også ændre oplysningerne.

Troldene kan nu se alle Annas private beskeder, fotos og aktivitetslog og de spreder det hele online. De finder også nogle personlige intime billeder på de konti, som kun var til hende og hendes kæreste. Nu bliver de sendt i omløb online.

## ARBEJDSSPØRGSMÅL

1. Bruger I den samme adgangskode til flere konti? Hvorfor?
2. Hvordan kan man sikre sine konti endnu bedre?

**TIP: Undersøg hvad password managers, multi-faktor-login og to-faktor-login er, og hvad det betyder for at have en god cyberhygiejne.**

3. Hvilke typer konti, kan man oprette?
   - lav en liste over de mange forskellige typer konti, som I tænker Anna, jer selv og andre unge nok har adgang til.
4. Er der forskel på hvilke konti, det er vigtigt at beskytte adgangen til? Er der nogen hvor sikkerhed og forsigtighed er vigtigere end andre? Undersøg hvad den gamle talemåde "kæden er aldrig stærkere end sit svageste led" betyder, og tænk over, om det er relevant at bruge talemåden i en tid med online konti og adgangskoder.

### BRUG JERES VIDEN TIL EN INFORMATIONSKAMPAGNE

For at løse mission 2 skal I lave en informationskampagne – det kan eksempelvis være en plakat. I skal bruge den viden I har opsamlet i jeres arbejde med casen om Anna og troll-angrebet til at lave en plakat (eller et andet kommunikationsprodukt), der kan hjælpe andre til at få en bedre cyberhygiejne.

### INSPIRATION TIL BUDSKABER

I må selv bestemme, hvilket budskab I synes er det vigtigste at kommunikere.

I kan bruge følgende to eksempler til inspiration, eller finde på jeres eget:

1. Kampagnen skal få folk til at overveje, hvilke informationer de deler på sociale medier.
   Eller
2. Kampagnen skal få de trolde, der måske uden at tænke over det "mobber" online – til at overveje deres adfærd.

Forhåbentlig kan vi med jeres ideer til gode kampagner, nedsætte antallet af sager som Annas i fremtiden.

## JERES PRÆSENTATION

I skal nu forberede en præsentation af jeres arbejde med missionen og jeres produkt.
I præsentationen skal I:

- Kort redegøre for jeres mission, den viden I har fået og de refleksioner I har gjort jer omkring Annas case.
- Præsentere jeres informationskampagne (gerne med billeder, video, skærmoptagelse m.m.)
- Fortælle, hvordan I kom frem til jeres endelige informationskampagne
- Argumentere for, hvilken effekt I tror, at jeres kampagne kan få hos jeres målgruppe
- Fortælle, hvilke refleksioner eller ahaoplevelser, I har haft undervejs
- Præsentationen skal være kort og må max tage 5 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 upload funktionen på konkurrencens hjemmeside: https://cybermissionen.cyberskills.dk, hvor I kan læse mere.

CYBERMISSIONEN

# BEGREBSLISTE

## Hvor mange begreber kender I?

### TRUSSELSMODELLERING

Trusselsmodellering handler kort fortalt om at identificere sårbarheder i et system og dermed også uønskede hændelser, så man eksempelvis som udvikler af et stykke software kan være bedre forberedt.

### 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

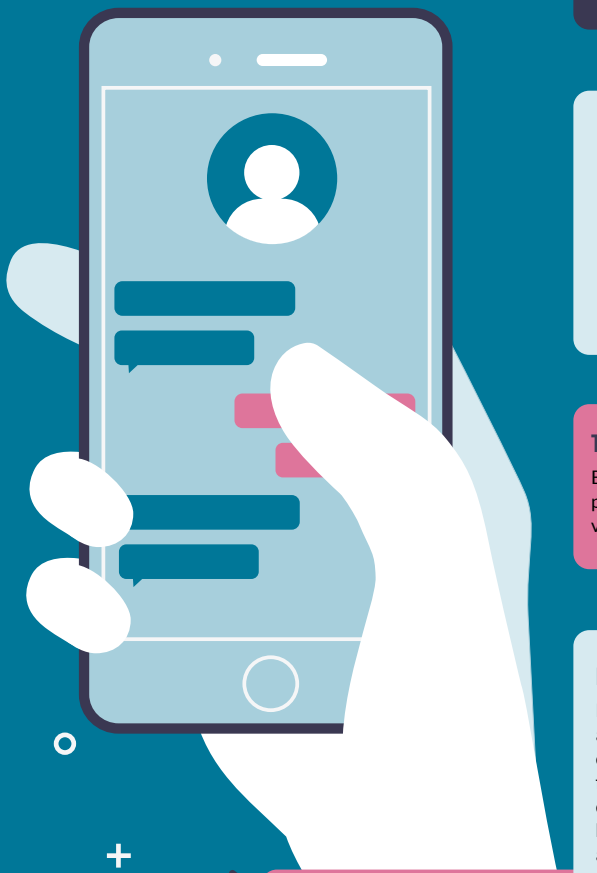
Mange virksomheder laver cyber awareness træning. Det kan eksempelvis være kommunikationsaktiviteter eller uddannelse, der skaber opmærksomhed om informationssikkerhed hos medarbejderne, så de får en mere sikker digital adfærd.

### 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.

### VULNERABILITY DISCLOSURE PROGRAM

En VDP giver etiske hackere klare retningslinjer for, hvordan de indberetter potentielt ukendte og skadelige sårbarheder til de organisationer, der står bag systemet.

### 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.

### TROLL

En troll (på dansk: internettrold) er en person, som bevidst forsøger at fremprovokere vrede og had på internettet.

### 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

BØRNE- OG
UNDERVISNINGSMINISTERIET
STYRELSEN
FOR IT OG LÆRING

CYBER SKILLS