|  |
| --- |
| Digital mobning og krænkelse – Niveau 2 |

Indhold

[Introduktion til forløbet 2](#_Toc79400750)

[Digital dannelse: 2](#_Toc79400751)

[Digital mobning: 3](#_Toc79400752)

[Digital krænkelse: 3](#_Toc79400753)

[Grooming: 3](#_Toc79400754)

[Hate speech: 4](#_Toc79400755)

[Deepfake: 4](#_Toc79400756)

[Opgaver 4](#_Toc79400757)

# Introduktion til forløbet

* 1. Læreren forklarer eleverne, at dette forløb har en varighed på 2\*45 minutter, og at det handler om digital dannelse.
	For ikke at male fanden på væggen ift. de unge mennesker kan du evt. overveje at gøre modulet til en del af et forløb, der omhandler flere forskellige perspektiver på det digitale – og eksempelvis bruge tid på at tale om, hvad fordelene er ved denne verden forud for forløbet
	2. *Hvis holdet allerede har haft første del af forløbet (niveau 1), springes begrebsafklaringen over, og der startes ved punkt e.*
	3. Begrebsafklaring: Hvad betyder
		1. **Digital dannelse**?
		2. **Digital mobning**?
		3. **Digital krænkelse**?
		4. **Grooming**?
		5. **Hate speech**?
		6. **Deepfake**?

# Digital dannelse:

Hvad betyder digital dannelse? Hvis vi splitter de to ord ad, har vi *digital*, som leder tankerne hen på noget, der omsætter noget fysisk til data, og altså er noget, man ikke umiddelbart kan røre ved. Og så har vi *dannelse*, som vel kan oversættes til noget i stil med: at man opfører sig ordentlig! Så altså: *digital dannelse* handler om, hvordan man opfører sig på forskellige medieplatforme, fx på internettet, i TV, i radioen og på telefonen. Det handler om vores adfærd i den verden vi bliver mere og mere en del af - den digitale og virtuelle.

Det handler om hvad vi gør, deler, forbruger, læser, ser og tror på - og hvordan vores kritiske sans, værdier og fornuft gør det muligt for os at navigere igennem den digitale verden på bedste måde. Forskellige teknologier gør det muligt at bruge apps til at manipulere multimodaliteter som lyd og billedredigering, sociale medier gør at vi har trolling, grooming og mobning. Det er også teknologier der, når de er brugt rigtigt, kan løse problemer for os og forbinde os med hinanden. Det er evnen til at forstå og bruge digitale medier. Det er evnen til at reflektere kritisk over digitale medier, deres indhold og opbygning. Det er evnen til at forstå, hvordan man opfører sig socialt acceptabelt på digitale medier.

## Digital mobning:

Først skal vi lige se på, hvad ordene dækker. Mobning: ”vedvarende og ondsindet drilleri, ofte mod et barn, udført af en eller især flere andre personer, ofte børn”. (DDO)

Digital mobning er, når en person bliver forfulgt, udelukket fra fællesskabet eller gjort grin med. Men digital mobning har nogle særlige kendetegn:

* Tonelejet, fordi man kan “gemme” sig bag skærmen
* Det foregår på alle tider af døgnet
* Mobberne kan være anonyme
* Beskeder om offeret kan cirkulere på de sociale medier i lang tid
* Ikke altid synlig for voksne

Det særlige ved digital mobning er, at man i det virtuelle rum kan sløre sin identitet, eller udgive sig for en anden. Man oplever derfor heller ikke mimikken eller reaktioner hos den man skriver til.

## Digital krænkelse:

Det at krænke betyder: ”*skade eller begå overgreb mod nogens ære, selvfølelse el.lign*.” Ibid.

Digital krænkelse betyder helt konkret krænkelser, der sker på internettet. Det er, når en person deler billeder eller video på nettet uden at have fået tilladelse eller samtykke. Billedet kan være delt af personen selv, men ikke givet tilladelse til at billedet må deles med andre.

Billeder kan også anskaffes gennem hacking, hvor en person på ulovlig vis har skaffet sig adgang til billeder.

## Grooming:

Grooming er det begreb, der bruges om den digitale børnelokker. Her er der en person, en voksen, som opsøger børn på digitale platforme og udgør sig for en jævnaldrende. Det er mest mænd, og de går efter at narre børnene eller barnet til seksuelle ydelser, enten digitalt eller via fysiske møder. Det er en person, der igennem en længere periode opbygger tillidsforhold til den unge med henblik på at begå overgreb mod barnet. Det sker gennem lange dialoger og ved brug af forskellige tricks. Det kan være svært at gennemskue, fordi groomerne er dygtige til deres formål. Sproget bliver tilpasset og opnår derved anerkendelse og status hos den unge. Det kan foregå både online og offline.

## Hate speech:

Hatespeech dækker over det begreb, der går ud på at håne eller umenneskeliggøre en person pga. fx race, køn, udseende, religion eller politiske overbevisning.

## Deepfake:

Deepfakes er et begreb, hvor der fremstilles falske videoer ved hjælp af kunstig intelligens. Det er noget, som er blevet brugt i de senere år, både på de sociale medier og traditionelle nyhedsmedier. Deepfake giver en ny dimension til fake news, hvor det bliver sværere end nogensinde at skelne mellem hvad der er ægte og falsk i nyhedsstrømmen.

# Opgaver

* 1. Efter hver begrebsforklaring skal det være muligt for eleverne at stille spørgsmål
	2. Der vises en lille film om digitale sexkrænkelser [[1]](#footnote-1), klassen deles op i grupper, som derefter arbejder med disse spørgsmål: (Skrives på tavlen eller deles på skærm)
		1. Hvad menes med ”uønsket sekularisering”?
		2. Er der forskel på krænkelser i den fysiske verden og den digitale verden? Forklar hvilke.
		3. Hvorfor synes de unge, at det er svært at forklare voksne om digitale krænkelser?
		4. Kan man anmelde digital krænkelse til politiet?
		5. Hvilke former for billeder er det ofte der bliver brugt til digitale krænkelser?
		6. Er der flest billeder af piger, der bliver delt uden samtykke, eller er der flest billeder af drenge?
		7. Hvem henvender sig mest til Red Barnet angående digital krænkelse: Piger eller drenge? Hvorfor?
	3. De ovennævnte opgaver diskuteres efterfølgende i plenum, og der skal gives plads til, at eleverne selv bidrager (hvis de ønsker det), evt. hjulpet i gang med indledende spørgsmål: Kender I nogen, som ……?
	4. Individuel opgave: Hver elev skal nu bruge en computer og åbne dette link: [Digitale krænkelser - Hvad er det? - Digitalt Ansvar](https://digitaltansvar.dk/fokusomraader/digitale-kraenkelser/). Eleven skal skrive svarene i Word og sende det til læreren, som senere kan give respons i det format, han/hun foretrækker. Opgaverne dertil lyder:
		1. Udover nøgenbilleder og -videoer er der flere andre områder, som også hører ind under digitale krænkelser. Nævn min. 5 eksempler.
		2. Beskriv med egne ord hvad ”hævnporno” betyder.
		3. Beskriv hvordan casen om digital chikane udlægges. Er Jens, 46 år, et offer eller en krænker? Begrund dit svar.
		4. Læs om Bismallahs case: ”Trusler på arbejdspladsen”, og skriv, hvad du ville råde hende til.
		5. Kig på grafen over ”Anmeldelser af digitale krænkelser på politi.dk” og forklar hvad den viser. Kom desuden med et bud på stigningen ved april 20.
		6. Forklar, hvad straffelovens § 264d, §235 og § 232 går ud på.
	5. Gruppearbejde: Klassen skal nu arbejde med fakta boksen i grupper. De skal lave en planche eller et Excel-ark, hvor de via et diagram viser nedenstående:



* 1. Se den lille film[[2]](#footnote-2) og snak derefter om i plenum, HVAD de unge i interviewet siger om de voksnes holdninger til det at dele intime billeder på nettet. Er du enig?
	2. Snak om hacking – og hvordan man bedst beskytter sine konti på nettet

Når vi laver kodeord, hopper vi ofte over hvor gærdet er lavest. Vi laver et kodeord vi ofte bruger, og fordi vi så ikke skal huske på alt for mange kodeord. Men det gør det nemmere for hackere at knække din kode. Hackere der vil have adgang til dit kodeord, anvender en række forskellige teknikker og metoder for at få adgang.

**Forceringsangreb**: Her gætter hackeren løs på hvad dit kodeord kan være. De bruger ordbøger for at kigge på kodeord fra hackede websites. Men heldigvis er det sådan i dag, at man får mail om at der er forsøgt at blive logget ind, og det har været forkert

**Keyloggers:** Her gemmer din computer dine anslag, hvilket gør det nemt for hackere at installere en keylogger på hans maskine og skabe forbindelse til din computer, for så at se hvilke taster du bruger.

**Social Engineering:** her prøver hackeren at gætte dit kodeord ud fra din profil på Facebook, LinkedIn eller andre sociale medier. Mange har nemlig tendens til at bruge oplysninger som fødselsdage, partners eller børnenes navne og adresser som kodeord, fordi de er nemme at huske.

* **Så hvordan kan du beskytte dig?**Der er mange metoder hackere bruger for at få uautoriseret adgang til systemer som mail, intranet osv. Derfor er der heller ikke kun en metode til at sikre dig og dine systemer.
* Men en af de gode råd er, en password manager, som er et program der hjælper med at huske dine kodeord – og ikke mindst kan hjælpe med at skabe sikre kodeord.
* Et andet råd er 2-faktor-godkendelse, som der bruges sammen med password manager. 2-faktor-godkendelse er hvor du får en SMS eller gennem en app får en tidsbegrænset kode der skal anvendes for at få adgang til tjenesten. Dette er med til at forhindre en hacker i at få adgang, fordi du modtager besked, hvis nogen forsøger at logge ind.

**Simple råd til et stærk kodeord**

* Brug et langt kodeord – jo længere jo bedre (helst 12 tegn eller mere)
* Brug ikke almindelige ord, som findes i ordbogen
* Brug ikke tal og bogstaver i rækkefølge (f.eks. 123456 eller abcde)
* Brug ikke tal og bogstaver i den rækkefølge de er på tastaturet (f.eks. qwerty)
* Gentag ikke tal og bogstaver (f.eks. 111, aaa)
* Udskift ikke tegn med åbenlyse erstatninger (f.eks. 0 i stedet for o, 3 i stedet for E)
* Brug ikke det samme kodeord på forskellige websites
* Brug ikke tekst og tal som kan gættes ud fra din profil på de sociale medier
* Hold øje med de web-adresser, hvor du indtaster dit kodeord
* Brug en VPN-forbindelse, når du anvender offentlige wi-fi-netværk
	1. Quiz
	2. Evaluering
	3. Ekstra materiale, som kan lægge op til forskellige opgaveformer, alt efter niveau:
		1. [https://deepfakelab.theglassroom.org/index-da\_DA.html](https://eur04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdeepfakelab.theglassroom.org%2Findex-da_DA.html&data=04%7C01%7Ctir%40fgunordvest.dk%7C8dcfd3279dee4eac9a5408d8e78a85f0%7Cfc1bab000e864f53a9a2e2e944031b4c%7C1%7C0%7C637513929436081233%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=Ig6zvmxGAxxsLd0QjWI96Rc4H%2FkbJLY%2Bm4yV4miQuec%3D&reserved=0)
		2. [https://www.youtube.com/watch?v=cQ54GDm1eL0](https://eur04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DcQ54GDm1eL0&data=04%7C01%7Ctir%40fgunordvest.dk%7C8dcfd3279dee4eac9a5408d8e78a85f0%7Cfc1bab000e864f53a9a2e2e944031b4c%7C1%7C0%7C637513929436101226%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=FYiCJd9awdkjfmiTpxXD9xyyIgFGAwXWetHL%2F2KA6DQ%3D&reserved=0)
		3. [https://www.youtube.com/watch?v=VhFSIR7r7Yo](https://eur04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DVhFSIR7r7Yo&data=04%7C01%7Ctir%40fgunordvest.dk%7C8dcfd3279dee4eac9a5408d8e78a85f0%7Cfc1bab000e864f53a9a2e2e944031b4c%7C1%7C0%7C637513929436101226%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=42wAkt%2BhCyU8F3oWfsQhVoyCdemoY2uViHU67H63ZRg%3D&reserved=0)
		4. [https://www.youtube.com/watch?v=1OqFY\_2JE1c](https://eur04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D1OqFY_2JE1c&data=04%7C01%7Ctir%40fgunordvest.dk%7C8dcfd3279dee4eac9a5408d8e78a85f0%7Cfc1bab000e864f53a9a2e2e944031b4c%7C1%7C0%7C637513929436111218%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=dc3ErzskE7QkNWIg4Ldg%2B%2B39MZVmI6Qy%2Fkzq8srofhE%3D&reserved=0)



Digital Mobning og krænkelse Modul 2

Elev evaluering af ovenstående forløb via nedenstående link eller QR-kode:

<https://surveys.enalyzer.com?pid=2s6gup5k>



1. [Hvad er en digital krænkelse? - Danske Gymnasier](https://www.danskegymnasier.dk/hvad-er-en-digital-kraenkelse/) (varighed 9,16 minutter) [↑](#footnote-ref-1)
2. [Deling af billeder - Det Kriminalpræventive råd (dkr.dk)](https://dkr.dk/it/deling-af-billeder/) (varighed 4,36 minutter) [↑](#footnote-ref-2)