

Holdningspapir for DIGITAL DANNELSE I DET DANSKE SAMFUND

Rådet for Digital Sikkerhed ønsker at tilskynde arbejdet med, at sikre den bedst mulige generelle digitale dannelse blandt alle samfundets borgere. Det er vores overbevisning, at det er nødvendigt at etablere et generelt højere niveau af digital dannelse blandt danske borgere. Det skal ske i sammenspil med andre målrettede digitale tiltag (som fx mere effektiv vidensdeling & uddannelse af flere cybersikkerhedsspecialister), som forankres i en samlet koordineret indsats. Kommunerne og de kommunale institutioner rustes til at påtage sig et større ansvar for at fremme digital ansvarlighed og digital dannelse. Det bør ske i samspillet mellem den Nationale Cybersikkerheds Strategi og den Fælles Offentlige Digitaliseringsstrategi.

For at vi som samfund kan nyde godt af digitaliseringens muligheder er det afgørende, at danskerne har styr på de basale råd om sikker digital adfærd, men også at vi evner at bruge og kritisk reflektere over brugen af digitale løsninger.

Samlet set vil det have den nødvendige positive effekt på den samlede informationssikkerhed og derfor er det en god investering ikke bare for den enkelte, men også for virksomheder, offentlige organisationer, uddannelsesinstitutioner og samfundet bredt set.

Rådet for Digital Sikkerhed mener, det kræver en bred indsats på tværs af samfundslag, generationer, sektorer etc. og Rådet har bl.a. udarbejdet en række gode råd, der kan danne grundlag for sådanne indsatser.

Indledning

Vi står overfor nogle helt særlige udfordringer, når samfundet digitaliseres. Digital dannelse er vigtig, for at vi kan udnytte de mange muligheder digitaliseringen tilbyder, og ikke mindst når vi færdes og kommunikerer digitalt. Truslerne ved at færdes online er mange¹ og spænder fra identitetstyveri, phishing/smishing og online-afpresning til digitale sexkrænkelser (misbrug af billeder, spredning af intime billeder, romance-scams mm), snyd via digitale fupbutikker, fake news mv. Dette trusselsbillede understreger vigtigheden af en indsats på tværs af samfundslag, generationer, sektorer etc.

Som i den analoge del af samfundet er det vigtigt at forstå spillereglerne.

Når man anvender fx transportmidler (private såvel som offentlige), bør man kende færdselsreglerne, køreplanerne, de socialt accepterede spilleregler i trafikken mm. Vi tager som samfund ansvaret for at sikre disse kompetencer hos alle borgere/brugere. Dermed minimeres risikoen for at sætte fordelene over styr og borgere bliver ofre for ulykker, skuffelser, tab af tryk, sikkerhed osv.

Debatten om digital dannelse bør på tilsvarende vis handle om, at vi tager ansvar for, at alle gennem en højere grad af generel digital dannelse, opnår den samme tryk og forståelse indenfor det digitale univers som det analoge. Det kræver en investering, både som samfund og som borger.

Nærværende holdningspapir beskriver Rådet for Digital Sikkerheds forståelse af digital dannelse samt komme med bud på, hvilke indsatser Rådet mener, der er behov for, for at fremme vores digitale dannelse.

Digital dannelse

Digital dannelse handler om at have gode vaner, når man færdes digitalt og have teknologiforståelse og kompetencer, der understøtter sikker og kritisk færden på nettet. Digital dannelse handler om at have styr på og grundlæggende forståelse af:

1. **Sikker adfærd digitalt:** Handler fx om sikker brug af kodeord, sikring af wi-fi, at have styr på, opdateringer og back up. Her kan kendskab til metoderne bag cyberkriminalitet hjælpe borgerne til

¹ <https://sikkerdigital.dk/borger/trusler/>

at forstå og genkende digitale angreb, når de møder dem. Cyberkriminalitet er oftest berigelseskriminalitet, og ligesom de fleste mennesker instinktivt forstår at beskytte sig mod fx lommetyve, ved at opbevare pung og mobil sikkert, når man befinder sig et befærdet sted, vil man også kunne lære at sikre sine digitale værdier, når man bevæger sig online.

2. Digitale fodspor og online identitet. Man skal have en forståelse for de digitale fodspor, man sætter ved sin færden på nettet, brug af sociale medier og andre digitale produkter. Hvor deler man egne og andres oplysninger, herunder billeder, hvilke informationer har apps adgang til og ikke mindst, hvordan – hvis overhovedet muligt – begrænser eller sletter man sine spor og sikrer sit privatliv digitalt.

Hvis tjenesten er gratis, er det ofte, fordi man betaler med sine data eller der er mulighed for at opleve salg i app'en. Data kan her betyde fx personoplysninger, forbrugs- eller adfærdsmønstre, tekniske oplysninger om eller tilknyttet udstyr og lokationsdata, der kan benyttes til f.eks. profilering, målrettede reklamer og målrettet meningsdannelse², udvikling af kunstig intelligens og produktraffinerings. Endelig er der tjenester der tilbydes gratis for blot at have adgang til brugerens online platforme med henblik på at kunne påvirke personens holdninger eller adfærd i en bestemt retning. Her er også forståelse af cookies væsentlig: Cookies sørger for, at hjemmesiden fungerer, andre gemmer informationer om din adfærd på nettet for at give dig målrettede reklamer.

3. Kildekritik og fake news: Fake news, trolling, deep fakes og morgendagens nye manipuleringsteknologier udgør en stigende trussel mod demokratiet, der kun modsvares af en øget kildekritik og refleksion fra forbrugeren. Man har brug for en kritisk sans, når man f.eks. handler på nettet, søger informationer, læser nyheder eller deler indhold på de sociale medier³.

4. Forståelse af rettigheder

Apps og services som sociale netværk, udbydere af mailtjenester, musiktjenester, videotjenester, m.fl. har mange data om os – det kan fx være lokationsdata eller oplysninger om ens alder, geografiske bevægelsesmønstre, tilknytning til organisationer eller interessefællesskaber, der kan behandle oplysninger om følsomme forhold (race, religion, politik, helbred m.v.). Som forbruger har man en række rettigheder som fx retten til at vide, hvordan informationer om dig behandles.

5. Digital ansvarlighed: Ligesom man er ansvarlig for sin opførsel i det analoge samfund, er man ansvarlig for sin opførsel online. Det kan indebære, at man kommunikerer på samme måde i kommentarspor, som man ville ansigt til ansigt, at man forstår at der sidder rigtige mennesker i den anden ende af kommunikationen, at man ikke lader sig tirre af trolls, og at man forstår at lovgivningen også gælder online. Det sidste er især relevant i forhold fx deling af billeder af, eller oplysninger om, andre mennesker, og at trusler og injurier er lige så ulovlige online som offline.

² Det giver relevante reklamer, men er problematisk fx når den målrettede reklame fra spil-sider/alkohol producenter målrettes folk, der psykologisk set har nemt ved at blive afhængige

³ <https://videnskab.dk/kultur-samfund/hvad-er-digital-dannelse>

Rådet for Digital Sikkerhed ønsker en balanceret, men bred indsats

Der er behov for at øge indsatsen generelt i samfundet for bl.a. at sikre en bedre forståelse af ovenstående elementer af digital dannelse. Sådanne indsatser *kan* bestå af én eller flere af følgende aktiviteter:

- Et IT sikkerheds kørekort, som kan være motor for etablering af den brede digitale dannelse.
 - Rådet for Digital Sikkerhed deltager gerne i udviklingen heraf og er bekendt med, at der findes platforme, som relativt hurtigt kan implementeres som grundlag for en sådan aktivitet.
- Koordineret indsats for fremme af sikkerhedskulturen på arbejdspladser.
 - Herunder medvirken til et 'Road show' med undervisning i aktuelle trusler, herunder fokus på medarbejdere der har behov for særlige forholdsregler, m.v. og medarbejdere, hvor de har adgang til systemer og data hos deres arbejdsgiver.
 - Uanset hvor mange tekniske foranstaltningerne der iværksættes, bliver sikkerheden aldrig bedre end de brugere, som anvender teknologien.
 - Videreudvikling af sikkerhedstjekket og roadshow som sikrer, at især de mindre og mellemstore virksomheder tager nogle af de mange sikkerhedstilbud som organisationer og myndigheder bidrager til
- Etablering af cybersikkerhed og ansvarlig brug af digitale tjenester i alle relevante uddannelser, både som speciale, men også bredere i både folkeskole, ungdomsuddannelser og videregående uddannelser.
 - Etablering af communities for unge med interesse for cybersikkerhed, så de får mulighed for at dygtiggøre sig og bidrage til de cyberkompetencer Danmark har så hårdt brug for
- Folkeoplysning og uddannelse af befolkningen i sikker it-adfærd
 - Etablering af en sikkerhedsuge fx i ugen før vinterferien, idet det falder sammen med Safe Internet Day (9.2.2021)⁴
 - Digitaliseringsstyrelsen & Erhvervsstyrelsens tiltag med [Sikkerdigital.dk](https://www.sikkerdigital.dk), Medierådet for Børn og Unges mange forskellige initiativer til at understøtte forældre og fagprofessionelle i arbejdet med digital dannelse⁵.
 - og Forbrugerrådet Tænk og TrygFondens app Mit digitale selvforsvar er et godt grundlag.
 - Kampagner skal øge bevidstheden om og anvendelsen af ovenstående eksisterende tiltag.
 - Udvide scenarier med oplysning om fx:
 - privatlivsbeskyttelse i brug af apps, browsere, sociale medier, IoT enheder mm.
 - 'fake news', 'deep fakes' og generel sund kildekritik
 - Gode råd til forældre til 'de digitalt indfødte'

Hvad gør Rådet for Digital Sikkerhed

Rådet for Digital Sikkerhed arbejder for at udbrede kendskabet til it-sikkerhedsrisici og øge opmærksomheden omkring tiltag, der kan øge sikkerhedsberedskabet i såvel professionelt, som privat regi. Vi udarbejder løbende undervisningsmateriale, vejledninger og værktøjer i samarbejde med en række

⁴ <https://www.saferinternetday.org/>

⁵ <https://www.medieraadet.dk/medieradet/digitaldannelse>

interessenter på området, med det mål at støtte en balanceret tilgang til informationssikkerhed – og derigennem også at være med til at skabe bedre digital dannelse.

Rådets 7 vigtigste gode råd om digitale dannelse, ses her nedenfor:

1

HUSK KILDEKRITIKKEN

- Vær kildekritisk når du læser og deler historier og nyheder på sociale medier – er afsenderen et anerkendt nyhedsmedie eller en obskur blog? Hvad er afsenderens agenda?

2

UNDGÅ DELING UDEN TILLADELSE

- Del aldrig billeder eller informationer om andre uden specifik tilladelse. Det kan være både etisk forkert og decideret kriminelt.

3

RYD OP PÅ DINE SOCIALE MEDIER

- Dan overblik over dine oplysninger på sociale netværk og andre digitale platforme. Ryd op med jævne mellemrum.

4

TJEK DINE PRIVATLIVSINDSTILLINGER

- Tjek dine privatlivsindstillinger i browsere, apps, sociale medier og andre digitale produkter du bruger og vælg sikrest mulige indstillinger

5

DEL KUN DET ALLERMEST NØDVENDIGE

- Giv aldrig flere oplysninger end højst nødvendigt når du tilmelder dig nye services. Vær kritisk i forhold til om modtageren reelt har behov for specifikke oplysninger inden du udfylder alt.

6

TÆNK OVER AT INTERNETTET ALDRIG GLEMMER

- Holdningsindlæg og kommentarer lever evigt videre såfremt du ikke sletter dem aktivt (og selv da kan de for længst være kopieret). Skriv aldrig noget som du ikke ønsker en fremtidig arbejdsgiver skal se.

7

TÆNK OVER AT INTERNET KOMMUNIKATION ER ANDERLEDES

- Husk at du taler til rigtige mennesker når du har online dialoger. Det skrevne ord er let at misforstå, så tænk over dit ordvalg og undgå f.eks. ironi og sarkasme.