København, den 29. november 2023

Ekspertgruppe om kunstig intelligens og digital svindel

Syv anbefalinger til at ruste Danmark bedre mod digital svindel

Digital svindel er et voksende problem. Tal fra Det Kriminalpræventive Råd viser, at cirka 150.000 danskere i 2022 blev ofre for digital svindel, mens antallet af personer, der blev *forsøgt* svindlet, var endnu højere. Antallet af anmeldelser til politiet om digital kriminalitet er ligeledes vokset støt de senere år. Det har store personlige konsekvenser for de ramte i form af fx økonomiske tab eller tyveri af identitet. Intet tyder på, at udviklingen er ved at vende, og det stiller krav om en fortsat stærk og velkoordineret forebyggelsesindsats på området.

Behovet forstærkes af den hastige udvikling inden for kunstig intelligens (AI). På meget kort tid har nye værktøjer, drevet af såkaldt generativ AI, gjort sit indtog i danskernes hverdag. Med AI kan vi skrive tekster, generere billeder, efterligne stemmer og føre samtaler med computeren på en så naturtro måde, at det er umuligt at skelne fra virkeligheden. Den nye udvikling inden for kunstig intelligens tilbyder virksomheder, myndigheder og borgere hidtil uanede muligheder, som vi skal formå at bruge på en positiv måde.

Desværre kan den også misbruges af kriminelle til at udføre mere avanceret digital svindel. Vi ser allerede ekstremt overbevisende svindelmails, og eksempler på manipulerede billeder og stemmeefterligninger. Den generative AI kan føre til endnu mere udbredt og mere overbevisende svindel, og også helt nye typer af svindel i den digitale hverdag.

Det er vigtigt, at der bliver sat ind med det samme for at adressere denne udvikling og afbøde negative konsekvenser. Vi ser det som væsentligt for at fastholde trygheden og tilliden i danskernes digitale hverdag.

Derfor har vi identificeret syv anbefalinger til tiltag, som vi opfordrer alle private og offentlige aktører til at tage fat på straks. Både hver for sig og i fællesskab. Tiltagene er en blanding af nye og en styrkelse af eksisterende indsatser.

Vi står som samlet aktørkreds bag disse anbefalinger. Vi vil hver især bidrage til at realisere dem gennem arbejdet i vores egne organisationer og i de mange samarbejder, vi er en del af.

1: Indsats for øget opmærksomhed på digital svindel

Bevidstheden er lav blandt almindelige danskere om, hvor hastigt nye former for digital svindel opstår, og hvordan trusselsbilledet skifter blandt andet som følge af AI. Vi har brug for langt større fokus på digital svindel, hvordan den rammer den enkelte, og hvordan den hele tiden udvikler sig og opdager nye sårbarheder hos både private borgere og virksomheder. Såvel virksomheder som borgere i alle aldre skal rustes til at forstå og agere i forhold til digital svindel. Der er ligeledes brug for at styrke opmærksomheden blandt offentlige myndigheder og private virksomheder om, hvordan deres kommunikation kan gøre det vanskeligere for digitale svindlere at lokke danskere i fælden. Vi foreslår derfor, at udviklingen inden for AI bør være et selvstændigt fokusområde inden for denne oplysningsindsats i takt med, at problemet udvikler sig i Danmark. Risikoen for digital svindel skal kommunikeres på en måde, så den styrker trygheden og tilliden til teknologi og digitalisering, herunder AI. Den skal skabe forståelse for, at digital svindel kan ramme alle – ikke kun særligt udsatte grupper.

2: Udvikling af nye løsninger der forhindrer svindel

Tekniske løsninger kan spille en vigtig rolle i kampen imod digital svindel. For eksempel har indførelse af såkaldt tofaktorbekræftelse ved handel på nettet gjort en positiv forskel for omfanget af den økonomiske svindel. Der skal fortsat investeres i nye tekniske løsninger, der kan dæmme op for svindel, fx filtre og monitoreringsværktøjer. Muligheden for at anvende AI i disse løsninger skal undersøges. Det kan også være nødvendigt at udfordre hastigheden, hvormed digitale handlinger skal ske, fx ved udvikling af deponeringsløsninger med indlagt ventetid til kontrol eller bekræftelse af ægthed. I udviklingen af nye løsninger er der brug for at se fordomsfrit på nuværende regler, hvad der teknisk er muligt og vil være effektivt og hensigtsmæssigt, samt på hvem der skal udvikle og eje løsningerne for at sikre størst mulig grad af tillid til dem.

FORBRUGERRÅDET tænk

TrygFonden

 # 3: Styrket koordinering mellem offentlige og private organisationer

Mange offentlige myndigheder og private virksomheder og organisationer er allerede involveret i at beskytte danskernes digitale sikkerhed og investerer løbende ressourcer i kommunikation, nye værktøjer og tekniske løsninger. De mange gode indsatser bør koordineres i endnu højere grad end i dag, så de understøtter og forstærker hinanden bedst muligt. Det kan fx ske ved at samle beslutningskraft i eksisterende samarbejdsfora. Der er behov for, at regeringen afklarer, hvor dette ansvar forankres, og sikrer ressourcer til at løfte arbejdet. En styrket koordinering bør omfatte en fælles strategi for at holde øje med, hvordan det digitale trusselsbillede udvikler sig, hvilke tekniske løsninger der kan bringes i spil, og hvordan borgerne bedst hjælpes til at passe på sig selv og deres nærmeste. Lokale aktører, der er tæt på danskernes hverdagsliv, fx skoler, biblioteker og borgerservicecentre, bør ligeledes involveres mere i forebyggelsesindsatsen. Det samme gælder aktører, der hjælper andre i nære fællesskaber, såsom foreninger, lokale netværk og klubber.

 # 4: Koordinering af myndighedsansvar

Regeringen har fordelt ansvaret for digital sikkerhed på flere forskellige ministerområder. Hjemmesiden Sikkerdigital.dk samler kommunikation og værktøjer til borgere og virksomheder på tværs af myndighedsområder, hvilket er væsentligt for at sikre én indgang til information om digital sikkerhed. Der er fortsat behov for, at placeringen af ansvaret for regulering og indsatser vedrørende digital sikkerhed, herunder risici forbundet med kunstig intelligens, afklares og tydeliggøres. Dette vil styrke forudsætningerne for mere effektiv koordinering og bedre samarbejde mellem myndigheder, private virksomheder og organisationer.

 # 5: Øget forsknings- og vidensindsats

Set i lyset af den hastighed, hvormed løsninger baseret på kunstig intelligens udvikler sig, er der brug for at styrke viden om og forskning i teknologiens anvendelse. Det gælder i særlig grad viden om, hvordan AI bliver – og i fremtiden kan blive – brugt til kriminalitet, hvilke konsekvenser det kan have for tryghed og tillid i samfundet, samt viden om mulige løsninger, der kan imødegå de negative konsekvenser. Der er brug for en styrket, tværfaglig forsknings- og vidensindsats med det formål at styrke grundlaget for at sætte ind imod digital kriminalitet. Der er samtidig brug for gennem uddannelse op opkvalificering at sikre, at vi har de rette og nødvendige ressourcer og kompetencer på området i fremtiden.

 # 6: Styrket deling af informationer om digitale trusler mellem private og offentlige aktører

Opdaterede informationer og viden om aktuelle trusler fra digitale kriminelle er spredt ud over en lang række private og offentlige aktører. Der er brug for at dele, samle og kvalificere disse data. Det skal sikre grundlaget for at træffe bedre og hurtigere beslutninger, så der kan sættes ind på tværs af aktører imod nye trusler, så snart de opstår. Et bedre datagrundlag vil også kunne styrke mulighederne for forskning på området.

 # 7: Bekæmp digital svindel internationalt

Digital svindel er et grænseoverskridende problem. Udviklingen af værktøjer baseret på generativ AI, der kan generere naturtro tekst og tale på dansk, risikerer at forstærke den grænseoverskridende trussel. En del af den digitale svindel foregår via de store teknologivirksomheders platforme og services, såsom sociale medier og beskedtjenester. Det er nødvendigt, at internationale virksomheder og techgiganterne lever op til deres ansvar for at beskytte brugerne på deres platforme mod svindel. Dette kan bedst ske gennem en styrkelse af EU-samarbejdet, hvor der bør arbejdes på, at EU-lovgivning på det digitale område adresserer digital svindel i det nødvendige omfang.

Følgende organisationer står bag anbefalingerne:

Forbrugerrådet Tænk
TrygFonden
Finans Danmark
Ældre Sagen
Dansk Erhverv
Dansk Industri
IDA
IT-Branchen
Rådet for Digital Sikkerhed
Forsikring & Pension
Teleindustrien

FORBRUGERRÅDET tænk

TrygFonden