VEJLEDNING

Råd til særligt udsatte eller eksponerede grupper ifm. læk af personoplysninger

Tænk sikkerhed, hvis du kan være udsat pga. job, familieforhold, viden eller lignende

Styrelsen for Samfundssikkerhed

Indhold

Generelt om rådene og eksponerede eller udsatte persongrupper 3
Råd særligt til dig, der kan være i fare for vold, stalking og trusler 3
Overvej hemmelig adresse og telefonnummer 4
Beskyt dine personlige oplysninger på sociale medier 4
Sikker brug af it og IoT i dit hjem og hverdag 4
Vær opmærksom – og forberedt på forsøg på digital svindel 5
Sikkerhed i hjemmet 6
Vær opmærksom på, at CPR ikke bør være nok som bevis på, hvem du er.....7

Generelt om rådene og eksponerede eller udsatte persongrupper

Uvedkommende har skaffet sig uautoriseret adgang til personlige oplysninger, herunder navn, adresse og CPR-nummer gennem CPR-registret i september 2026. På den baggrund kan der være grupper af borgere, som er mere eksponerede for forsøg på svindel eller chikane ved brug af deres cpr-nummer.

Lækket medfører, at personer blandt disse eksponerede eller udsatte persongrupper skal have en større opmærksomhed på blandt andet deres omgivelser, adfærd på sociale medier og sikkerheden i deres hjem. Styrelsen for Samfundsikkerhed har samlet en række råd til personer, der kan være i en eksponeret eller udsat persongruppe efter læk af personoplysninger.

Rådene kan også gøre sig gældende ved øvrige hændelser, hvor der har været læk af personoplysninger.

Selvom man måske ikke tidligere har haft navne- og adressebeskyttelse, kan læk af CPR betyde, at man nu ønsker at beskytte sig yderligere fremadrettet og styrke sikkerheden omkring sine personlige oplysninger.

Det kan eksempelvis være, hvis man:

- har oplevet chikane tidligere
- har et arbejde, der kan være interessant for kriminelle
- har et navn, der kan sætte en i risiko for chikane eller sættes i forbindelse med udsatte sociale, etniske eller religiøse minoriteter
- er en offentlig kendt person, hvis navn kan misbruges

Råd særligt til dig, der kan være i fare for vold, stalking og trusler

Hvis du kan være i fysisk fare, fordi en bestemt person nu potentielt kender din adresse, bør du overveje:

- om navne- og adressebeskyttelse er relevant
- om politi, krisecenter, Dansk Stalking Center eller anden specialiseret rådgivning bør kontaktes
- om arbejdsplads, skole, institution eller andre relevante aktører bør orienteres.

Hvis du er bekymret for din sikkerhed som følge af lækkede personoplysninger, herunder hvis du allerede har navne- og adressebeskyttelse, kan du kontakte politiet på 1-1-4.

Ved akut fare skal du ringe 1-1-2.

Overvej hemmelig adresse og telefonnummer

Overvej at få navne- og adressebeskyttelse. Det kan fx være gavnligt, hvis du står over for en flytning.

Overvej derudover at få skjult, hemmeligt eller udeladt telefonnummer. Ved skjult nummer fremgår dit telefonnummer ikke hos andre i forbindelse med opkald. Med hemmeligt og udeladt nummer holdes oplysninger ude af offentlige teletjenester, nummeroplysning og online telefonbøger. Kontakt dit teleselskab for nærmere information.

Vær opmærksom på, at nogen kan finde på at bruge de lækkede oplysninger til at prøve at anskaffe sig flere oplysninger om dig. Hvis nogen allerede kender dit navn, din adresse og dit CPR-nummer, kan de misbruge oplysningerne til at udgive sig for være en troværdig person eller autoritet med henblik på at vinde din tillid og derigennem få dig til at videregive flere oplysninger om dig selv, fx dit arbejde. Det kan foregå både ved opkald, mails, kontakt på sociale medier eller ved fysisk kontakt.

Beskyt dine personlige oplysninger på sociale medier

På internettet, især på sociale medier, kan der ligge mange personlige oplysninger om dig, som andre ikke nødvendigvis bør kunne tilgå. Disse oplysninger kan sammen med CPR-oplysninger bruges af udvedkommende til chikane eller identitetstyveri. For at begrænse andres adgang til dine private eller følsomme oplysninger bør du derfor overveje, at:

- oprette en privat profil på sociale medier, hvor du kun deler privat indhold med en snæver kreds
- oprette, hvis nødvendigt, en professionel profil, som er adskilt fra din private. Brug gerne en professionel mailadresse, der er adskilt fra dine private aktiviteter, til den professionelle side
- være opmærksom på, hvor mange private eller følsomme oplysninger, der ligger offentligt tilgængeligt på dine profiler og sider. Ryd eventuelt op i gammelt indhold eller brug privatlivsindstillingerne til at begrænse synligheden for offentligheden
- undlade at dele billeder eller oplysninger, der kan bruges til at identificere din privatadresse eller din arbejdsplads
- bede familie og venner om ikke at dele oplysninger om dig eller billeder af dig uden dit samtykke
- oprette flerfaktor-autentificering på alle relevante profiler
- skifte passwords, hvis du har mistanke om, at de er kompromitteret i fx datalæk eller hvis de er genbrugt eller svage, fx fordi de er korte eller helt eller delvis er baseret på navn, adresse og/eller CPR-nummer
- være ekstra opmærksom på venneanmodninger på sociale medier. Kig fx efter, om personen er verificeret.

Sikker brug af it og IoT i dit hjem og hverdag

Hvis du oplever at være udsat i forhold til, at dit it-udstyr kan blive kompromitteret, kan det være en god ide at opdatere din computer, mobil og øvrigt udstyr såsom router. Skift også password på computer, mobil, router mm, hvis dit, navn, adresse eller CPR-nummer indgår.

Du kan også overveje at slå lokationstjenester såsom Google Maps, Apple Maps og Snap Map i Snapchat fra, så man ikke kan se, hvor du befinder dig.

Hvis du har videoovervågning, som er koblet på internettet, bør du være opmærksom på, at mange IoT-enheder (Internet of things), herunder videokameraer, udleveres med standard-loginoplysninger. Hvis du ikke allerede har ændret brugernavn og passwords, så bør du gøre det nu. Standard-loginoplysninger kan findes på internettet, og er dermed nemme at hacke.

Vær opmærksom – og forberedt på forsøg på digital svindel

Læk af personoplysninger fra CPR-registeret kan misbruges i forbindelse med svindel. Det giver svindlere viden om dig på forhånd, som de kan bruge til at virke troværdige ved telefonisk kontakt eller via mail. Derfor opfordres du til at udvise agtpågivenhed. På Sikkerdigital.dk har Styrelsen for Samfundssikkerhed som følge af lækket af CPR-oplysninger samlet en række generelle råd til, hvordan man som borger forebygger svindel med personoplysninger:

Gode råd til forebyggelse af digital svindel fra Sikkerdigital

Vær ekstra opmærksom på uventet kontakt
I den følgende tid skal du være særlig opmærksom på sms'er, opkald og mails, hvor afsenderen bruger CPR-oplysninger om dig. Det samme gør sig gældende ved henvendelser på sociale medier.

Klik ikke på uventede links
Hvis du modtager uventede sms'er eller mails med links, så klik ikke, men gå selv ind via den officielle hjemmeside – eller ring til afsenderens hovednummer og dobbelttjek.

Del ikke oplysninger
Del aldrig MitID-oplysninger, engangskoder, adgangskoder eller kortoplysninger.

Ved konkret mistanke om svindel: Opret en kreditadvarsel på borger.dk
Ved konkret mistanke om svindel med dit CPR-nummer, kan du oprette en kreditadvarsel. Kreditadvarsel er en markering i CPR, der gør det sværere at optage lån eller kredit i dit navn.

På Sikkerdigital.dk kan du se, hvordan du gør i en trin-for-trin-guide på siden her.

Benyt ikke dit CPR-nummer som adgangskode
Hvis du benytter hele eller dele af dit CPR-nummer som adgangskode, så anbefaler vi at skifte det.

Du kan bevise din identitet med AltID
Du kan som borger risikere at blive mødt af højere krav til legitimation. Staten tilbyder et sikkert digitalt legitimationskort, som du kan hente i appen AltID. Det er Danmarks officielle app til id og beviser. Med appen kan du bevise din identitet uden at dele unødige oplysninger om dig selv.

Myndigheder og banker beder dig aldrig om at oplyse personlige oplysninger over mail, telefon eller ved fysisk fremmøde på din bopæl.

Vær desuden opmærksom på, om der på MitID fremgår anmodninger om godkendelser, som du ikke genkender. Hvis du er det mindste i tvivl, skal du altid afvise anmodningen og kontakte den relevante myndighed eller virksomhed via dennes officielle kontaktoplysninger.

Hvis du opdager noget mistænkeligt via fx MitID, er det vigtigt, at du har en procedure klar, så du kan reagere hurtigt og kontakte rette vedkommende.Hvis du fx oplever konkret misbrug, kan det, afhængig af hændelsen, være relevant at:

- kontakte banken ved økonomiske transaktioner
- kontakte MitID Support og eventuelt spærre MitID, hvis der faktisk er tegn på kompromittering
- kontrollere relevante konti og kontaktoplysninger
- etablere kreditadvarsel på borger.dk
- kontakte virksomheder, hvor identiteten er blevet misbrugt
- gemme dokumentation som sms'er, mails, telefonnumre og breve
- anmelde misbruget til politiet

Du kan få hjælp ved at ringe til Cyberhotline for digital svindel på 33 37 00 37 på hverdage kl. 8-20 og i weekender og på helligdage kl. 10-16.

Bemærk, MitID bør ikke spærres alene, fordi CPR-nummer og adresse er lækket. Det er relevant ved *konkret* mistanke om misbrug af MitID.

Sikkerhed i hjemmet

For at sikre, at dit hjem kan være en tryg base, bør du overveje, hvorvidt det er hensigtsmæssigt at dele din privatadresse med fremmede fx via sociale medier eller ved at lægge billeder op på sociale medier, der viser, hvor du bor.

Hvis du føler dig utryg, kan du også overveje at sikre dit hjem. Det Kriminalpræventive Råd har på sin hjemmeside samlet gode råd til, hvordan du kan gøre dette i praksis.

Gode råd fra Det Kriminalpræventive Råd vedrørende sikring af bolig

På dkr.dk kan du blandt andet læse om, hvordan du sikrer,

- at dine vinduer, døre og låse er robuste i din bolig,
- at der er belysning omkring huset, som er sensorstyret,
- at der er etableret hegn og beskåret hæk eller anden beplatning, så det ikke kan dække for uvedkommende

I den forbindelse kan det også være relevant at tilmelde sig Nabohjælp som indbrudsforebyggende tiltag med henblik på at sikre sig selv og sine naboer.

Hvis du har været udsat for hærværk eller chikane ved din bolig, kan du desuden overveje at opsætte kameraovervågning, som du også kan læse mere om på Det Kriminalpræventive Råds hjemmeside dkr.dk.

Hold generelt øje med unormal adfærd omkring din bolig, og overvej om naboer kan hjælpe med at holde øje. Hvis du føler dig utryg i eget hjem, kan du overveje, om der er mulighed for at bo ved familie, venner eller andet for en periode.

Hvis du bliver udsat for situationer, der har karakter af strafbare handlinger, opfordres du til at kontakte politiet på 1-1-4 på det sted, hvor handlingen har fundet sted. Er du i akut fare, skal du ringe 1-1-2.

Vær opmærksom på, at CPR ikke bør være nok som bevis på, hvem du er

Vær opmærksom på, at du ikke længere alene bør kunne valideres på CPR-nummer. Hvis en myndighed ringer og oplyser dit CPR-nummer, kan du lægge på og efterfølgende selv ringe til myndigheden eller virksomheden via et officielt nummer. Brug ikke selv dit CPR-nummer i din henvendelse til myndighederne, eksempelvis i telefonen, hvis du kan gøre det via sikker post eller lignende.

Hvis du har børn

Tænk også på børnenes oplysninger. Undgå at offentliggøre:

- børnenes skole eller institution
- adresse
- faste rutiner, som fx fritidsinteresser
- billeder, der viser lokalområdet
- oplysninger om, hvor I opholder jer

Hvis din sikkerhedssituation involverer en tidligere partner eller anden konkret person, bør du også fortælle relevante personer omkring børnene om situationen.

Styrelsen for Samfundssikkerhed

Datavej 20
3460 Birkerød
+45 45 16 16 66

Cyberhotline for digital sikkerhed

Cyberhotline for digital sikkerhed er til borgere og virksomheder, som ønsker vejledning om, hvordan de bliver mere digitalt sikre samt håndterer og forebygger digital svindel og cyberangreb. Som borger kan du få hjælp, hvis din identitet er blevet misbrugt.

Ring 33 37 00 37