

FOLKETINGSVALG

Sikker adfærd for opstillede kandidater

Marts 2026



Styrelsen for
Samfundssikkerhed

Indhold

Digital sikkerhed	4
Udenlandske påvirkningsaktiviteter	7
Fysisk chikane og trusler	9

Forord

Denne folder er til dig, der stiller op til folketingsvalget 2026, og som ønsker mere viden om, hvordan du kan beskytte dig selv mod chikane, trusler, digitale angreb og påvirkningsvirksomhed.

Med en god sikkerhedsadfærd beskytter du ikke kun dig selv – du beskytter også opretholdelsen af et demokratisk og retfærdigt folketingsvalg.

Digital sikkerhed

En stor del af det politiske virke foregår online. Du tjekker mails, laver opslag på sociale medier og bruger it-systemer. Brugen af digitale tjenester er dog forbundet med en vis risiko, som du som kandidat bør forholde dig til. I dette afsnit kan du læse om, hvad du kan gøre for at styrke din digitale sikkerhed.

Beskyt adgangen til dine konti

Personer med ond hensigt kan forsøge at få adgang til dine konti på sociale medier, e-mailtjenester og andre systemer bl.a. for at få fat i følsomme oplysninger eller for at stille dig i et dårligt lys. For at gøre det svært for andre at få adgang, kan du:

- Lave stærke passwords på minimum 15 tegn.
- Bruge forskellige passwords til forskellige systemer, tjenester og platforme.
- Aktivere multifaktor-autentifikation, hvor det er muligt. Multifaktor-autentifikation er et ekstra lag af sikkerhed, hvor du – ud over brugernavn og adgangskode – bruger en ekstra bekræftelsesmetode til at bevise, at det rent faktisk er dig, der logger ind. Det kan eksempelvis være via fingeraftryk, autentifikationsapp, bekræftelsesmail m.m.
- Bruge www.haveibeenpwned.com til at tjekke om dine loginoplysninger har været en del af et datalæk og ligger frit tilgængeligt for uvedkommende online. Hvis dette er tilfældet, bør du skifte dit password.
- Bruge en passwordmanager til at holde styr på dine passwords.

Pas på phishing

Phishing er forsøg på at manipulere dig til at videregive personlige eller følsomme oplysninger. Det kan foregå både via mail, opkald og sms'er. Ofte vil personen bag et phishing-angreb udgive sig for at være en autoritet og forsøge at få dig til at klikke på fx links til falske hjemmesider eller åbne inficerede filer. For at minimere sandsynligheden for phishing-angreb kan du:

- Sørge for ikke at klikke på links i e-mails eller sms'er. Gå i stedet ind på hjemmesiden tilhørende den organisation, der har sendt dig e-mailen eller sms'en.
- Afbryde kontakten, hvis der i en besked eller et opkald opfordres til at dele følsomme oplysninger.
- Være særligt opmærksom på beskeder eller opkald, hvor du opfordres til at reagere hurtigt.
- I forbindelse med et telefonopkald fortælle personen, der har ringet dig op, at du kontakter dem via hovednummeret, lægge på og derefter selv ringe dem op via det officielle hovednummer.

Mobile enheder

Mobiltelefoner og tablets er nødvendige redskaber både privat og arbejdsmæssigt. Men de er også sårbare over for digitale angreb. For at styrke din digitale sikkerhed på dine mobile enheder kan du:

- Anvende passwords på alle mobile enheder.
- Opdatere dine mobile enheder, så snart du får en notifikation om en ny opdatering.
- Sørge for kun at installere apps fra officielle tjenester, eksempelvis App Store eller Google Play.

Offentligt wi-fi

Offentlige wi-fi kan designes og udnyttes af hackere til at opsnappe datatrafikken til og fra din pc eller mobile enhed. På den måde kan de få adgang til følsomme oplysninger om dig. For at beskytte dig selv, kan du bruge din telefons mobildata til internetdeling.

Hvis du af forskellige årsager alligevel har brug for at benytte et offentligt wi-fi, kan du installere og benytte en VPN-løsning til at kryptere trafikken.

Beskyt dine personlige oplysninger på sociale medier

Personer med onde hensigter kan have interesse i at finde og misbruge personlige oplysninger om dig. På internettet, især på sociale medier, ligger ofte mange personlige oplysninger om dig, som andre ikke nødvendigvis skal kunne tilgå. For at begrænse andres adgang til dine private eller følsomme oplysninger kan du:

- Oprette en privat profil og en professionel side på sociale medier, så du kun deler privat indhold med en snæver kreds, men deler fagligt indhold med offentligheden. Brug gerne en professionel mailadresse, der er adskilt fra dine private aktiviteter, til den professionelle side for blandt andet at mindske risikoen for at blive omfattet af datalæk af passwords.
- Være opmærksom på, hvor mange private eller følsomme oplysninger, der ligger offentligt tilgængeligt på dine profiler og sider. Ryd op i gammelt indhold eller brug privatlivsindstillingerne til at begrænse synligheden for offentligheden.

I forbindelse med påvirkningsoperationer er der set eksempler på, at der er blevet oprettet profiler i politikeres navne for på den måde at fremstå legitim og misbruge profilen til at sprede desinformation. For at undgå, at dit navn misbruges til at sprede desinformation, kan det være en god idé at oprette profiler på de sociale medier, hvor du endnu ikke er oprettet. På disse profiler kan du henvise til din hjemmeside og oplyse, at profilen ikke benyttes aktivt. Husk at monitorere profilerne for at sikre, at de ikke bliver kompromitteret.

Hvor det er muligt, bør dine konti på sociale medier verificeres. På den måde er det synligt for brugerne, at det sociale medie har verificeret, at du er den reelle ejer af kontoen.

Cyberhotline for Digital Sikkerhed og Sikkerdigital.dk

Læs mere om digital sikkerhed, herunder stærke passwords, multifaktor-autentifikation samt brug af wifi og VPN, på www.sikkerdigital.dk eller ring til Cyberhotlinen for Digital Sikkerhed på 33 37 00 37.

Udenlandske påvirkningsaktiviteter

I de seneste år har der været flere eksempler på, at fremmede stater har forsøgt at påvirke den almene meningsdannelse og politiske beslutningsprocesser i Vesten. Påvirkningsaktiviteterne pågår kontinuerligt, og formålet med fremmede staters påvirkningsaktiviteter er overordnet set at underminere samfundets sammenhængskraft og fremme egne interesser.

Påvirkningsaktiviteter foregår både via platforme på internettet og gennem påvirkningsagenter. Påvirkningsagenter er personer, der arbejder sammen med fremmede efterretningstjenester med henblik på at skabe og udnytte relationer i udlandet i påvirkningsøjemed.

Truslen fra påvirkningsaktiviteter mod folketingsvalget 2026

På Styrelsen for Samfundssikkerheds hjemmeside kan du læse om truslen fra påvirkningsaktiviteter mod folketingsvalget 2026: <https://samsik.dk/publikation/truslen-fra-paavirkningsaktiviteter-mod-folketingsvalget-2026>

Vær opmærksom på påvirkningsagenter

Fremmede stater forsøger bl.a. at opbygge relationer til politikere ved at invitere dem til konferencer. Dette gør de for på et senere tidspunkt at kunne udnytte relationen i sin påvirkningsvirksomhed.

Som folketingskandidat er det vigtigt, at du er bevidst om truslen fra ulovlig påvirkning. Du bør være opmærksom på, om de personer eller organisationer, som ønsker at samarbejde med dig, har gode intentioner, eller om de kunne have et skjult motiv.

Undgå at sprede des- og misinformation

Fremmede stater spreder falske og vildledende historier for at påvirke dit verdensbillede og skabe splittelse i vores samfund. For at beskytte dig selv og vores demokrati er det derfor vigtigt, at du forholder dig kritisk til, hvad du læser og hører. Det kan du gøre ved at følge disse tre råd:

Stop op

Falske og vildledende historier blander sig med pålidelige nyheder og opslag på sociale medier, og det kan være svært at skelne. Samtidig spiller fremmede stater ofte på vores følelser for at manipulere os. Derfor er det vigtigt, at du stopper op og giver dig tid til at forholde dig kritisk til, hvad du læser og hører. Spørg dig selv:

- Appellerer historien med vilje til stærke følelser, fx vrede eller frygt?
- Kan historien være vildledende eller have en skjult hensigt?
- Kan historien være plantet for at afspore debatten, så tvivl om fakta eller skabe mistillid til myndigheder, politikere eller befolkningsgrupper?

Tænk efter

Fremmede stater fabrikere falske og vildledende historier for at få dig til at dele dem. Historierne får især effekt, når de i god tro deles af almindelige mennesker. Når historien deles af en, du kender, bliver det sværere at gennemskue historiens troværdighed. Gør det til en vane at holde en pause, før du deler historier, især på sociale medier. Spørg dig selv:

- Kan jeg stå inde for indholdet? Har jeg læst teksten igennem, eller kan jeg komme til at dele noget, som jeg ikke helt kan stå inde for?
- Hvem kan have gavn af, at jeg deler denne historie?
- Bidrager jeg til splid eller konstruktiv dialog ved at dele historien?

Tjek kilden

Indhold på sociale medier bliver ikke faktatjekket, som det gør i traditionelle nyhedsmedier. På sociale medier er det derfor relativt let at sprede falske og vildledende historier, som ligner troværdigt indhold. Derfor er det vigtigt, at du tjekker afsenderen, og hvor historien kommer fra, inden du deler. Spørg dig selv:

- Hvem er afsender?
- Hvor kommer historien eller informationerne fra? Er det en pålidelig kilde?
- Findes historien andre steder end på sociale medier, fx i traditionelle nyhedsmedier?

Hvem former dine holdninger?

På Styrelsen for Samfundssikkerheds kampagnehjemmeside, www.vaerkritisk.dk, kan du læse mere om, hvordan du kan opdage og undgå at sprede fremmede staters falske og vildledende historier.

Fysisk chikane og trusler

Intimiderende adfærd kan omhandle fysiske krænkelser som spyt, slag, skub og spark. Men det kan også omhandle verbale overfald, som kan finde sted i det fysiske rum.

Selvom fysisk intimidering sjældent forekommer, er det vigtigt, at du som politiker tager højde for risikoen og er bevidst om, hvilke forholdsregler du kan tage for at forebygge og håndtere intimidering.

Hvis du bliver udsat for intimidering i en form, der har karakter af strafbare handlinger, opfordres du til at kontakte politiet på det sted, hvor handlingen har fundet sted.

Sikkerhed omkring offentlige aktiviteter

I forbindelse med offentlige aktiviteter, såsom debatarrangementer og vælgermøder, bør du være opmærksom på, om arrangementet har en dagsorden, som kan føre til tilspidsede diskussioner, eller som kan tiltrække stærkt utilfredse borgere eller personer fra ekstremistiske miljøer. Ved offentlige arrangementer, hvor du vurderer, at der kan være en høj risiko for konflikt, kan du overveje at lægge møderne på tidspunkter, hvor du kan få hjælp fra andre i bygningen og være opmærksom på, hvordan man hurtigt kan komme ud af lokalet.

Hvis du som folketingskandidat laver opsøgende aktiviteter såsom uddeling af flyers eller deltagelse i lokale aktiviteter, kan du overveje at gøre det sammen med andre.

Hvis du i forbindelse med offentlige aktiviteter oplever borgere, der virker vrede eller truende, kan du overveje, om du skal indgå i dialogen, eller om det er bedre at trække sig. For at vurdere hvorvidt en fortsat dialog er gavnlig, eller om det giver mest mening at trække sig, kan du benytte dig af følgende råd:

- Vurdér om der er overhængende fare for, at der kan opstå vold. Er du i umiddelbar fare, så forlad stedet og tilkald hjælp.
- Bevar et roligt kropssprog, og giv den anden person plads.
- Vær klar om dine grænser for, hvad du vil finde dig i. Både over for dig selv, men også over for modparten.

Sikkerhed i hjemmet

For at sikre, at dit hjem kan være en tryk base, kan du overveje, hvorvidt du deler din privatadresse med uvedkommende eller fx lægger billeder op på sociale medier, der viser hvor du bor. Vurdér ligeledes, om du skal have hemmelig adresse.

Hvis en borger opsøger dig på din privatadresse, er du ikke forpligtet til at åbne døren. Hvis du vælger at åbne døren for borgeren, kan du gå udenfor og foreslå, at I mødes og tager drøftelsen et offentligt sted på et andet og mere passende tidspunkt.

Det kan desuden være en god idé at overveje at sikre sit hjem som led i at beskytte sig selv. Du kan besøge Det Kriminalpræventive Råds hjemmeside og få gode råd til, hvordan du kan gøre dette. Rådene går blandt andet på, hvordan du kan sikre, at boligens vinduer, døre og låse er robuste, at der er belysning omkring huset, som er styret af en sensor og ikke mindst, hvordan nabo hjælp kan give tryghed. Hvis du har været udsat for hærværk ved din bolig, kan du overveje at opsætte kameraovervågning, som du også kan læse mere om på det Det Kriminalpræventive Råds hjemmeside.

Hvis du bliver udsat for situationer, der har karakter af strafbare handlinger, opfordres du til at kontakte politiet på det sted, hvor handlingen har fundet sted.

Sikring af dit hjem

På Det Kriminalpræventive Råds hjemmeside kan du læse om, hvordan du sikrer dit hjem som led i at beskytte sig selv: <https://dkr.dk/indbrud/indbrud-i-din-bolig>

Kontaktordning for folkevalgte og deres pårørende

Er du allerede valgt ind i Folketinget, en kommunalbestyrelse eller et regionsråd, er du omfattet af politiets kontaktordning for folkevalgte og deres pårørende. Kontaktordningen, som findes i alle Rigsfællesskabets politikredse, er en nem og direkte indgang til politiet, hvis du som folkevalgt eller pårørende til en folkevalgt oplever chikane, trusler eller andre utryghedsskabende hændelser relateret til dit politiske virke.

Kontaktordningen er et tilbud, hvor politiet yder vejledning og rådgivning, når folkevalgte eller deres pårørende har behov for at drøfte konkrete hændelser, bekymringer eller vil anmelde et forhold. Kontaktordningen kan også benyttes til mere generel vejledning om forebyggelse, tryghed og sikkerhed i relation til bl.a. chikane og trusler.

Hvis du ikke er omfattet af kontaktordningen, men oplever chikane, trusler eller andre utryghedsskabende hændelser, kan du kontakte politiet på telefon 114.

Kontaktordning for folkevalgte og deres pårørende

Folketingsmedlemmer og deres pårørende er omfattet af Københavns Politis Kontaktordning:

- Tlf.: 2939 5937
- E-mail: kbh-kontaktordning-folkevalgte@politi.dk

Læs mere om kontaktordningen for folkevalgte og deres pårørende på politiets hjemmeside, hvor det også fremgår, hvordan medlemmer af kommunalbestyrelser og regionsråd kan rette henvendelse til kontaktordningen: <https://politi.dk/demokrati>

Ved henvendelser anbefales det, at du oplyser, at du er folkevalgt eller pårørende til en folkevalgt, samt hvordan hændelsen eller bekymringen er relateret til dit eller din pårørendes politiske virke, så din henvendelse kan blive håndteret via kontaktordningen.

Ved henvendelser, der kræver akut udrykning fra politiet, ambulance, brandvæsen eller miljøberedskab, skal du ringe 112. Ved henvendelser af ikke-hastende karakter kan du ringe til politiets servicecenter på 114.



Styrelsen for
Samfundssikkerhed

Datavej 20
3460 Birkerød
+45 45 16 16 66

Rådgivning

Kontakt til Styrelsen for Samfundssikkerhed angående rådgivning om sikkerhed, cybersikkerhed og forsyningssikkerhed: raadgivning@samsik.dk

Pressekontakt

Kontakt til Styrelsen for Samfundssikkerhed for pressen, medier og journalister:
presse@samsik.dk
+45 23 23 63 00

Pressetelefonen har åbent alle hverdage fra kl. 9-16.