



VALG

Bokmål

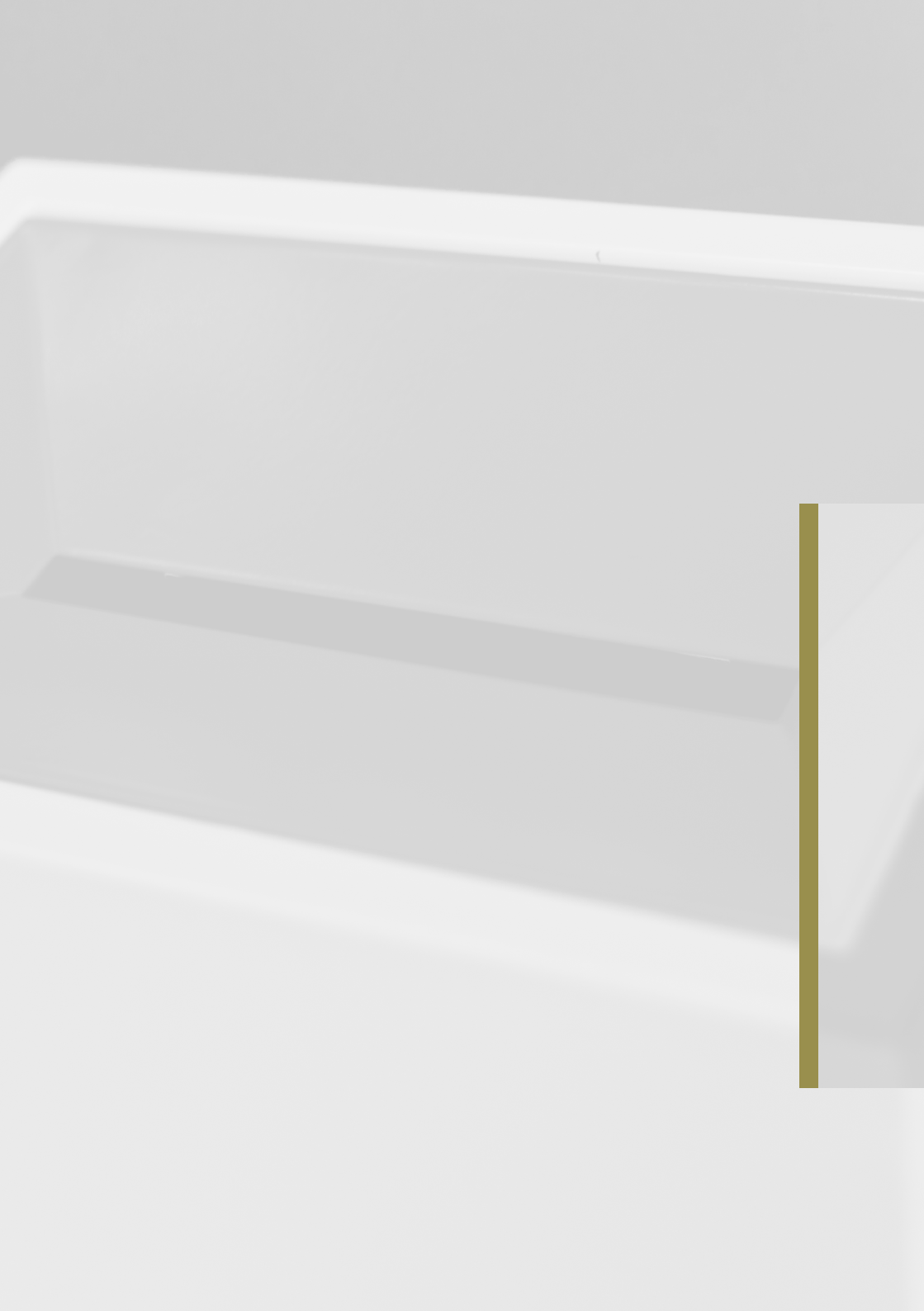
Stortings- og sametingsvalget 2025

Gode sikkerhetsråd til deg som stiller til valg



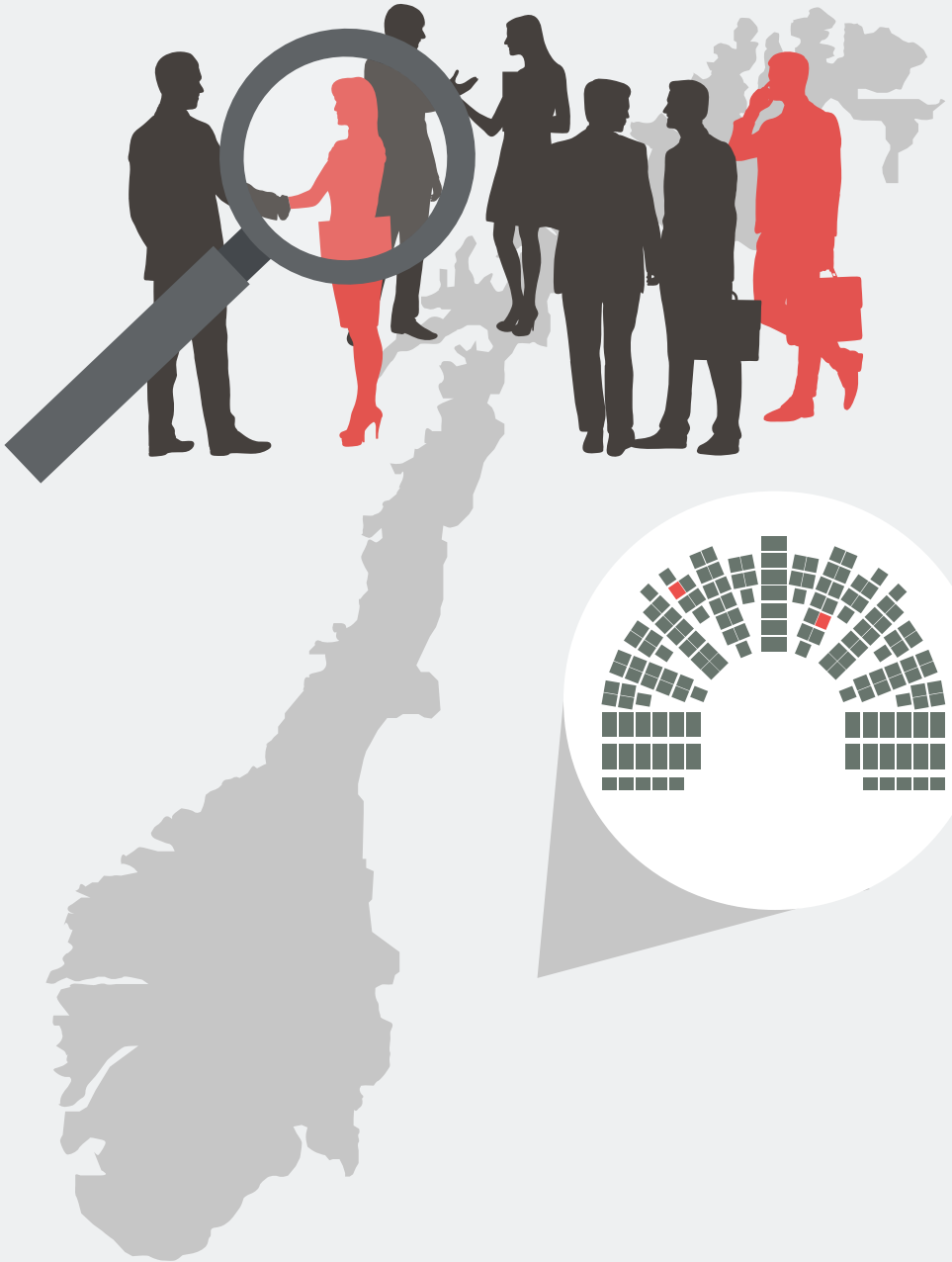
Utarbeidet av

- Etterretningstjenesten
- Nasjonal sikkerhetsmyndighet
- Politiets sikkerhetstjeneste



Innhold

Norge – et tillitsbasert samfunn	5
Din informasjon – ditt ansvar	5
Du er av interesse	5
Kjenn dine verdier	8
Når bør du be om rådgivning?	10



Norge – et tillitsbasert samfunn

Tillit er en sentral forutsetning for demokratiet. Denne tilliten er under press. Sammensatte trusler, som påvirkningsoperasjoner, kan ha som mål å skade tilliten demokratiet er bygget på. Desinformasjon og påvirkningsoperasjoner har vært fremtredende i flere valg i andre land de to siste årene.

Påvirkning kan rettes mot gjennomføringen av valget, mot politiske aktører eller mot velgerne og holdninger i befolkningen. Vi har et velfungerende og stabilt demokratisk system og et samfunn preget av åpenhet. Det bidrar til robusthet både i institusjonene og hos enkeltpersoner med politiske verv. Norge har dermed et godt utgangspunkt for å stå imot forsøk på slik påvirkning av innenrikspolitiske prosesser.

Samtidig skal vi ikke være naive. Fremmede stater vil kunne søke informasjon om og påvirke norske politikere, politiske prosesser eller forhold. Hver og en av oss kan bidra til å sikre sensitiv informasjon om oss selv og politiske prosesser, samt å håndtere eventuell påvirkning.

Din informasjon – ditt ansvar

Du må selv bidra til å beskytte egen informasjon og de verktøyene du bruker for å kommunisere. Hva du selv gjør har betydning for din sikkerhet og evne til å kommunisere trygt og sikkert. Det er viktig at du har kunnskap om hvordan du kan håndtere situasjoner som kan innebære risiko. Dette kan være situasjoner knyttet til menneskelige relasjoner og bruk av digitale verktøy.

Du er av interesse

Fremmede staters etterretningstjenester driver målrettede operasjoner i Norge. Særlig der man har motstridende eller konkurrerende interesser. Når du stiller til valg betyr det at du må regne med at fremmede staters etterretningstjenester kan være interessert i deg som et ledd i sin virksomhet. For å nå sine mål bruker de både åpne og skjulte metoder. Detaljert kunnskap om deg, både som privatperson og politiker, kan ha høy verdi. Etterretningstjenestene er dyktige til å skape relasjoner mellom mennesker, blant annet gjennom hyggelige og naturlige møter. Kunnskap om f.eks. sensitiv og privat informasjon, politiske standpunkt eller planer kan utnyttes. Noe så tilsynelatende enkelt som din kontaktliste på telefonen kan være av interesse.



E-POST

Det sendes stadig ut e-post som utgir seg for å være noe de ikke er. Avsenderne spiller på tillit, frykt eller fristelser. For eksempel at noen utgir seg for å være banken din og skal ha deg til å logge inn for å løse et problem. I det du klikker på en lenke eller åpner vedlegget øker risikoen for at enheten din kan overtas av andre, eller de får tak i påloggingsinformasjon eller annen viktig informasjon som kan utnyttets videre.



MENNESKELIG TILNÆRMING

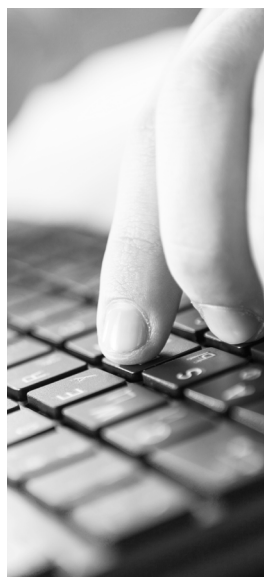
En norsk politiker kommer i snakk med en diplomat, delegasjonsmedlem eller næringsdrivende. Senere inviteres politikerens på lunsj. Lunsjen følges opp med flere møter over en lengre periode. Politikerens bes om informasjon om andre i partiet eller et konkurrerende parti. Det kan være av personlig karakter eller jobbrelatert. Vedkommende ber også politikerens legge til rette for møter med ledelsen i partiet eller andre interessante parter. Utenlandske aktører som nevnt i eksemplet kan være tilknyttet eller utnyttet av landets etterretnings-tjeneste. Dette er en vanlig måte å operere på i Norge.



Sårbarheter utnyttes

Fremmede stater og andre aktører forsøker kontinuerlig å ta seg inn i norske datasystemer for å hente ut informasjon, sabotere eller ta kontroll. Daglig blir mennesker lurt og digitale svakheter utnyttet.

En annen utbredt metode for å ta seg inn i datasystemer er å få deg til å åpne vedlegg eller lenker med skadevare i e-poster. E-postene kan se harmløse ut. Mer avanserte forsøk på å lure deg kan være e-poster som ser ut om de kommer fra en kjent avsender, mens den reelle aktøren bak er skjult. Du som stiller til valg må derfor aktivt jobbe for at dine digitale enheter og systemer har god sikkerhet. Du må være klar over at du kan bli forsøkt utnyttet som følge av ditt politiske virke. Vær derfor bevisst hvem du kontaktes av samt hvem du deler hvilken informasjon med.



Kjenn dine verdier



Vit hva som er verdifull informasjon for deg og ditt parti

- ▶ Hvilken informasjon har størst verdi eller alvorligste konsekvens for deg og ditt parti hvis andre fikk tilgang til den?
- ▶ Hvem kan du dele slik informasjon med og hvem skal den ikke deles med?



Behandle verdifull informasjon med forsiktighet

- ▶ Tenk over hva du skriver/sier hvor og hvem som leser/lytter – både på telefon og i det offentlige rom.
- ▶ Forsikre deg om identiteten til de du kommuniserer med.
- ▶ Enkelte temaer eller saker bør ikke diskuteres på telefon eller sendes via vanlig e-post eller SMS.
- ▶ Når noe er sensitivt, bør møter gjennomføres uten PC, mobil og smartklokker til stede.
- ▶ Bruk krypteringsløsninger for elektronisk kommunikasjon.



Beskytt ditt digitale utstyr og dine digitale tjenester

- ▶ Ikke lån bort dine digitale enheter til andre.
- ▶ Aktiver skjermlås, og bruk gjerne fingeravtrykk eller ansiktsgjenkjenning for å unngå at andre ser PIN-kode når du låser opp enheten.
- ▶ Hold digitale enheter oppdatert med siste versjon av apper/programvare.
- ▶ Bruk flerfaktor autentisering (bruk av passord i kombinasjon autentiseringsapp, kodebrikke eller lignende) der hvor det tilbys.
- ▶ Bruk forskjellige passord for hver tjeneste.



E-post

- ▶ Vær kritisk til lenker og vedlegg i e-post som du mottar.
- ▶ Er du usikker på om du bør åpne et vedlegg eller en lenke – vurder om det er strengt nødvendig.
- ▶ Ta kontakt med avsender via telefon/annet om du er i tvil.
- ▶ Gjør gjerne et internettsøk på informasjonen uten å åpne lenken/vedlegget.
- ▶ Rapporter mistenkelige e-poster til egen partiorganisasjon, tillitsvalgt for din liste eller arbeidsgiver.



Sosiale medier, apper og digitale tjenester

- ▶ Vær kritisk til hvilke apper og tjenester du installerer på dine digitale enheter.
- ▶ Bruk personverninnstillingene til å beskytte tilgang og synlighet etter ditt behov.
- ▶ Vær bevisst på hva du legger ut om deg selv og andre.
- ▶ Vær kritisk til det som kan være falske nyheter – unngå å spre videre.
- ▶ Slå av informasjon om hvor du befinner deg om du absolutt ikke trenger å bruke det.
- ▶ Benytt et unikt, sterkt passord og slå på flerfaktoraутентisering.



På reise

- ▶ Unngå å koble deg opp til offentlige trådløse nett. Bruk mobildata eller mobilt bredbånd.
- ▶ Unngå å lade digitale enheter via andres USB ladepunkter/tilkoblinger.
- ▶ Dersom du reiser til særlig utsatte land, bør du ikke ta med din vanlige mobiltelefon, PC eller nettbrett. Dette gjelder for eksempel land som Norge ikke har et nært sikkerhetspolitisk samarbeid med.

Når bør du be om rådgivning?

Ta kontakt med din partiorganisasjon, tillitsvalgt eller din arbeidsgiver om du skulle oppleve hendelser som:

- ▶ Mottak av e-poster som er spesielt mistenkelige
- ▶ Tekniske uregelmessigheter i digitalt utstyr
- ▶ Tap av digitalt utstyr som mobiltelefon, PC og nettbrett
- ▶ Tap av verdifull informasjon
- ▶ Uønsket tilnærming
- ▶ Misbruk av dine profiler i sosiale medier
- ▶ Spredning av falsk informasjon

Dersom du tror du er utsatt for et digitalt angrep, påvirkning eller uønsket tilnærming, bør du så raskt som mulig informere og diskutere saken med din nærmeste leder – enten det er arbeidsgiver eller i partiorganisasjonen.

For utfyllende sikkerhetsråd kan du lese PSTs sikkerhetshåndbok «Personlig sikkerhet» på [PST.no](https://pst.no).

Fortsatt bekymret? Ta kontakt med relevante myndigheter som Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) eller lokalt politi.

For mer informasjon om digital sikkerhet, besøk nettvett.no.

For mer informasjon om kritisk medieforståelse, besøk medietilsynet.no.

For mer informasjon om hatefulle ytringer, hets og trusler mot politikere, besøk hatogtrusler.no.





NSM



*Denne brosjyren er utarbeidet av
Etterretningstjenesten, Nasjonal
sikkerhetsmyndighet og Politiets sikkerhetstjeneste
på oppdrag fra Forsvarsdepartementet
og Justis- og beredskapsdepartementet,
koordinert og finansiert av Kommunal- og
distriktsdepartementet.*