



VAL

Nynorsk

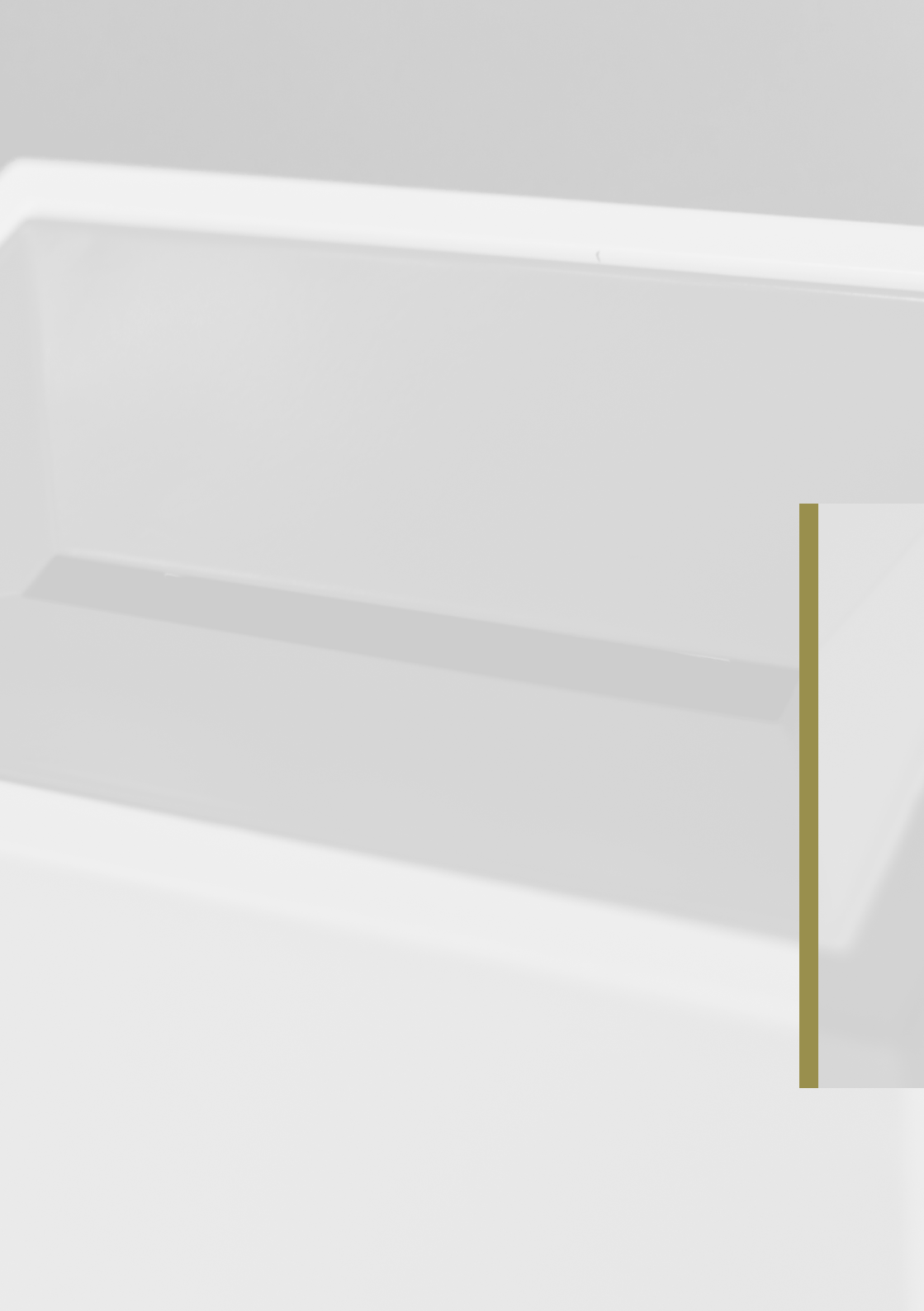
Stortings- og sametingsvalet 2025

Gode tryggingsråd til deg som stiller til val



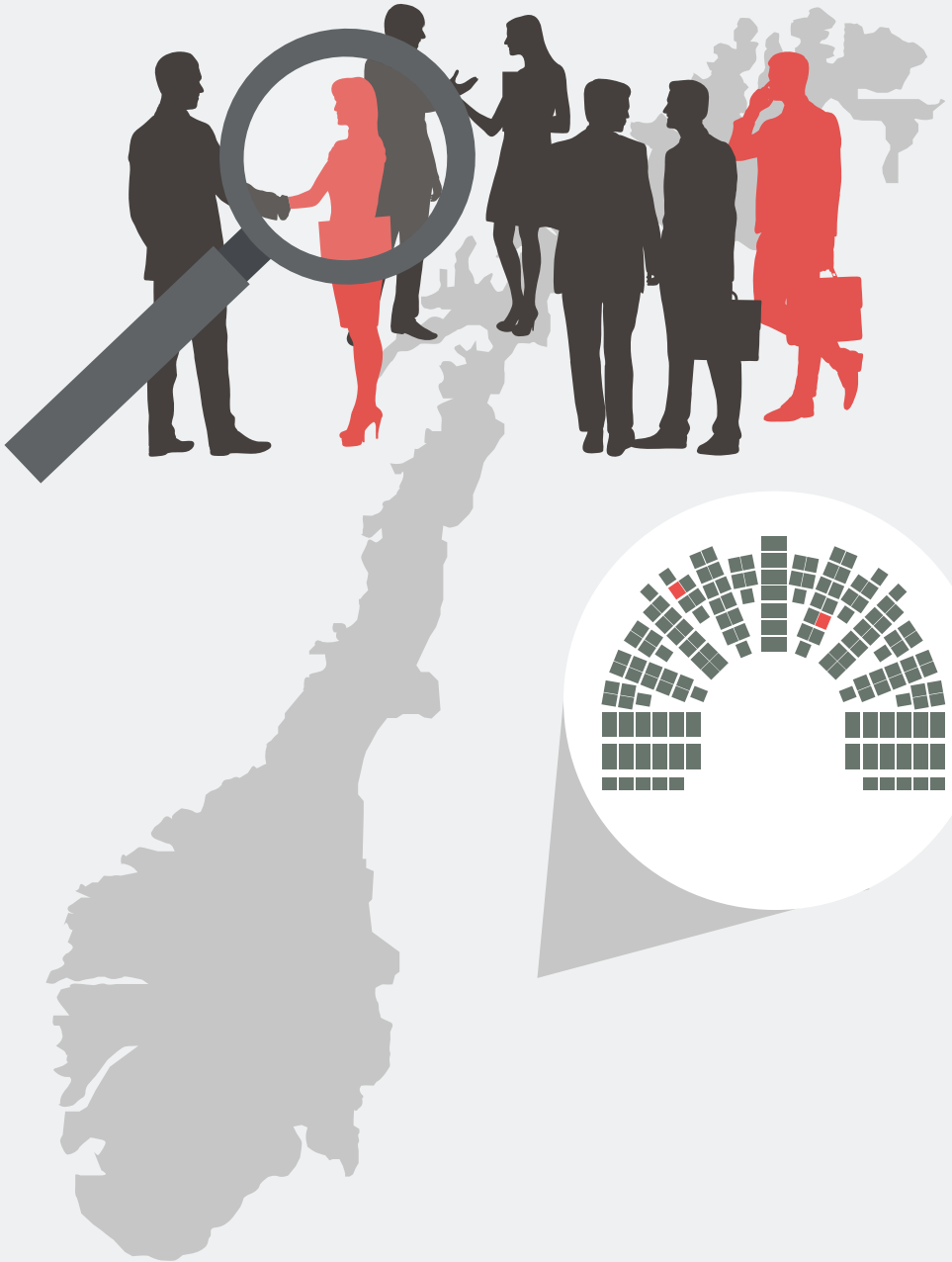
Utarbeidd av

- Etterretningstenesta
- Nasjonalt tryggingsorgan
- Politiets tryggingsteneste



Innhold

Noreg – eit tillitsbasert samfunn	5
Informasjonen din – ansvaret ditt	5
Du er av interesse	5
Kjenn verdiane dine	8
Når bør du be om rådgiving?	10



Noreg – eit tillitsbasert samfunn

Tillit er ein sentral føresetnad for demokratiet. Denne tilliten er under press. Samansette truslar, som påverknadsoperasjonar, kan ha som mål å skade tilliten demokratiet er bygd på. I fleire land har desinformasjon og påverknadsoperasjonar vore markante dei to siste åra.

Påverknad kan rettast mot gjennomføringa av valet, mot politiske aktørar eller mot veljarane og haldningar i befolkninga. Vi har eit velfungerande og stabilt demokratisk system og eit samfunn prega av openheit. Det bidreg til å gjere både institusjonane og enkeltpersonar med politiske verv robuste. Noreg har dermed eit godt utgangspunkt for å stå imot forsøk på slik påverknad av innanrikspolitiske prosessar.

Samstundes skal vi ikkje vere naive. Framande statar vil kunne søkje informasjon om og påverke norske politikarar, politiske prosessar eller forhold. Kvar og ein av oss kan bidra til å sikre sensitiv informasjon om oss sjølv og politiske prosessar, samt å handtere eventuell påverknad.

Informasjonen din – ansvaret ditt

Du må sjølv bidra til å beskytte din eigen informasjon og dei verktøya du brukar til å kommunisere. Kva du sjølv gjer, har betydning for tryggleiken din og evna di til å kommunisere trygt og sikkert. Det er viktig at du har kunnskap om korleis du kan handtere situasjonar som kan innebere risiko. Dette kan vere situasjonar knytt til menneskelege relasjonar og bruk av digitale verktøy.

Du er av interesse

Etterretningstenestene til framande statar driv målretta operasjonar i Noreg. Særleg der ein har motstridande eller konkurrerende interesser. Når du stiller til val, betyr det at du må rekne med at etterretningstenestene til framande statar kan vere interesserte i deg som eit ledd i verksemda si. For å nå måla sine bruker dei både opne og skjulte metodar. Detaljert kunnskap om deg, både som privatperson og politikar, kan ha høg verdi. Etterretningstenestene er dyktige til å skape relasjonar mellom menneske, blant anna gjennom hyggjelege og naturlege møte. Kunnskap om til dømes sensitiv og privat informasjon, politiske standpunkt eller planar kan utnyttast. Noko så tilsynelatande enkelt som kontaktlista di på telefonen kan vere av interesse.



E-POST

Det blir stadig sendt ut e-postar som gir seg ut for å vere noko dei ikkje er. Avsendarane spelar på til-lit, frykt eller freistingar. Til dømes kan det vere at nokon gir seg ut for å vere banken din og skal ha deg til å logge inn for å løyse eit problem. Idet du klikkar på ei lenkje eller opnar vedlegget, aukar risikoen for at eininga di kan over-takast av andre, eller dei får tak i påloggingsinformasjon eller annan viktig informasjon som kan utnyt-tast vidare.



MENNESKELEG TILNÆRMING

Ein norsk politikar kjem i snakk med ein diplomat, delegasjons-medlem eller ein næringsdrivande. Seinare blir politikaren invitert på lunsj. Lunsjen blir følgd opp med fleire møte over ein lengre periode. Politikaren blir beden om informasjon om andre i par-tiet eller i eit konkurrerande parti. Det kan vere av personleg karak-ter eller jobbrelatert. Vedkomande ber òg politikaren leggje til rette for møte med leiinga i partiet eller med andre interessante partar. Utanlandske aktørar som nemnt i dømet, kan vere knytte til eller utnytta av etterretningstenesta i landet. Dette er ein vanleg måte å operere på i Noreg.



Sårbarheiter blir utnytta

Framande statar og andre aktørar prøver kontinuerleg å ta seg inn i norske datasystem for å hente ut informasjon, sabotere eller ta kontroll. Dagleg blir menneske lurt og digitale sårbarheiter utnytta.

Ein annan utbreidd metode for å ta seg inn i datasystem på, er å få deg til å opne vedlegg eller lenkjer med skadevare i e-postar. E-postane kan sjå harmlause ut. Meir avanserte forsøk på å lure deg kan vere e-postar som ser ut som om dei kjem frå ein kjend avsendar, mens den reelle aktøren bak er skjult. Du som stiller til val må derfor aktivt jobbe for at dei digitale einingane og systema dine har god tryggleik. Du må vere klar over at nokon kan prøve å utnytte deg som følgje av det politiske virket ditt. Ver derfor medviten om kven du blir kontakta av og kven du deler informasjon med.



Kjenn verdiane dine



Vit kva som er verdifull informasjon for deg og partiet ditt

- Kva informasjon har størst verdi eller mest alvorleg konsekvens for deg og partiet ditt viss andre fekk tilgang til han?
- Kven kan du dele slik informasjon med, og kven skal han ikkje delast med?



Behandle verdifull informasjon med varsemd

- Tenk over kva du skriv/seier og kven som les/lyttar – både på telefon og i det offentlege rommet.
- Gjer deg trygg på identiteten til dei du kommuniserer med.
- Enkelte tema eller saker bør ikkje diskuteras på telefon eller sendast via vanleg e-post eller SMS.
- Når noko er sensitivt, bør møte gjennomførast utan PC, mobil og smartklokker til stades.
- Bruk krypteringsløysingar for elektronisk kommunikasjon.



Beskytt det digitale utstyret og dei digitale tenestene dine

- Ikkje lån bort dei digitale einingane dine til andre.
- Aktiver skjermlås, og bruk gjerne fingeravtrykk eller ansiktsgjenkjenning for å unngå at andre ser PIN-koden når du låser opp eininga.
- Hald digitale einingar oppdaterte med siste versjon av appar/programvare.
- Bruk fleirfaktoraautentisering (bruk av passord i kombinasjon med autentiseringsapp, kodebrikke eller liknande) der det blir tilbode.
- Bruk ulike passord for kvar teneste.



E-post

- Ver kritisk til lenkjer og vedlegg i e-post som du får.
- Er du uvisst på om du bør opne eit vedlegg eller ei lenkje, vurder om det er strengt nødvendig.
- Ta kontakt med avsendar via telefon/anna om du er i tvil.
- Gjer gjerne eit internettsøk på informasjonen utan å opne lenkja/vedlegget.
- Rapportert mistenkjelege e-postar til eigen partiorganisasjon, tillitsvald for lista di eller arbeidsgjevaren din.



Sosiale medium, appar og digitale tenester

- Ver kritisk til kva appar og tenester du installerer på dei digitale einingane dine.
- Bruk personverninnstillingane til å beskytte tilgjenge og synlegheit etter kva behov du har.
- Ver medviten om kva du legg ut om deg sjølv og andre.
- Ver kritisk til det som kan vere falske nyheiter – unngå å spreie dei vidare.
- Slå av informasjon om kvar du er, om ikkje du absolutt treng å bruke det.
- Bruk eit unikt, sterkt passord og slå på fleirfaktoraутентisering.



På reise

- Unngå å kople deg opp til offentlege trådlause nett. Bruk mobildata eller mobilt breiband.
- Unngå å lade digitale einingar via andre sine USB-ladepunkt/USB-tilkoplingar.
- Dersom du reiser til særleg utsette land, bør du ikkje ta med den vanlege mobiltelefonen, PC-en eller nettbrettet ditt. Dette gjeld til dømes land som Noreg ikkje har eit nært tryggingsspolitisk samarbeid med.

Når bør du be om rådgiving?

Ta kontakt med partiorganisasjonen din, tillitsvald eller arbeidsgjeveren din om du opplever hendingar som:

- ▶ Mottak av e-postar som er spesielt mistenkjelege
- ▶ Tekniske irregularetar i digitalt utstyr
- ▶ Tap av digitalt utstyr som mobiltelefon, PC og nettbrett
- ▶ Tap av verdifull informasjon
- ▶ Uønskt tilnærming
- ▶ Misbruk av profilane dine i sosiale medium
- ▶ Spreiing av falsk informasjon

Dersom du trur du er utsett for eit digitalt angrep, påverknad eller uønskt tilnærming, bør du så raskt som mogleg informere og diskutere saka med den næraste leiaren din – anten det er arbeidsgjevar eller i partiorganisasjonen.

For utfyllande tryggingsråd kan du lese PST si tryggleikshandbok «Personlig sikkerhet» på [PST.no](https://pst.no).

Er du framleis bekymra? Ta kontakt med relevante styresmakter som Politiets tryggingsteneste (PST), Nasjonalt tryggingsorgan (NSM) eller lokalt politi.

For meir informasjon om digital tryggleik, besøk nettvett.no.

For meir informasjon om kritisk medieforståing, besøk medietilsynet.no.

For meir informasjon om hatefulle ytringar, hets og truslar mot politikarar, besøk hatogtrusler.no.





NSM



*Denne brosjyren er utarbeidd av
Etterretningstenesta, Nasjonalt tryggingsorgan
og Politiets tryggingsteneste på oppdrag
frå Forsvarsdepartementet og Justis- og
beredskapsdepartementet, koordinert og finansiert
av Kommunal- og distriktsdepartementet.*