VAL

Nynorsk

Du er av interesse –

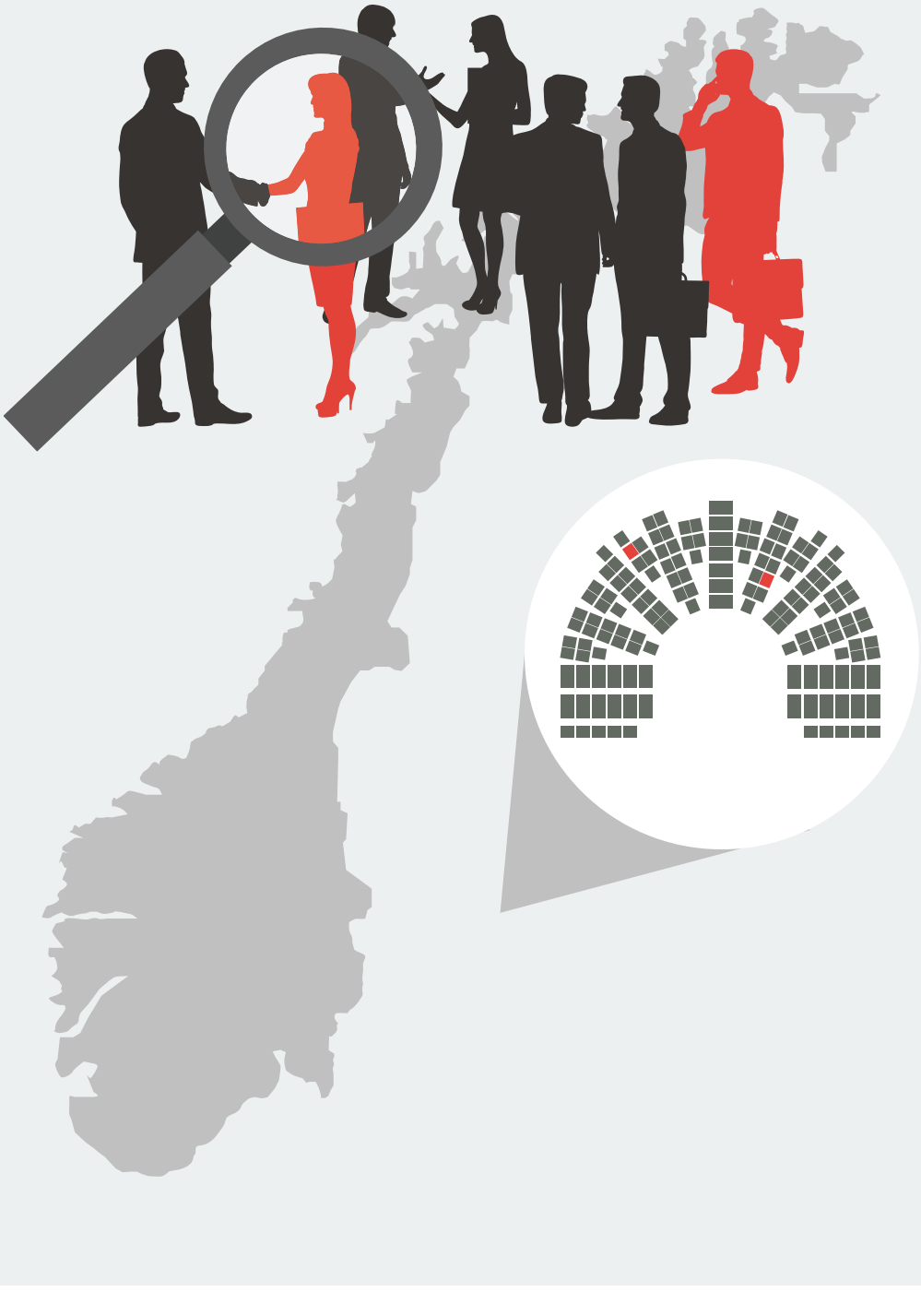
Gode tryggingsråd til deg som stiller til val

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

Det siste året har det vore auka merksemd rundt moglegheita for at både framande statar og ikkje-statlege aktørar prøver å påverke politiske prosessar i andre land. Påverknad kan i denne konteksta definerast som ein utanlandsk, statleg initiert (men gjerne gjennomført av ein ikkje-statleg aktør), fordekt og tilsikta aktivitet for å oppnå eit mål som på kort eller lang sikt kan svekkje norske interesser til fordel for ein annan stat.

Slik 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 kan søkje informasjon om og påverke norske politikarar, politiske prosessar eller forhold. Her kan kvar og ein av oss bidra til å sikre sensitiv informasjon om oss sjølv og om politiske prosessar og dessutan bidra til å handtere eventuell slik påverknad.

Informasjonen din – ansvaret ditt

Du må sjølv bidra til å beskytte eigen informasjon og dei verktøya du bruker for å kommunisere. Kva du sjølv gjer, har betydning for tryggleiken din og evna 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 knytte 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 konkurrerande 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. Noko så tilsynelatande enkelt som kontaktlista di på telefonen kan vere av interesse.

FALSK E-POST

Det blir stadig sendt ut e-postar som gir seg ut for å vere noko dei ikkje er. Avsendarane spelar på tillit, 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 overtakast av andre, eller dei får tak i påloggingsinformasjon eller annan viktig informasjon som kan utnyttast vidare.

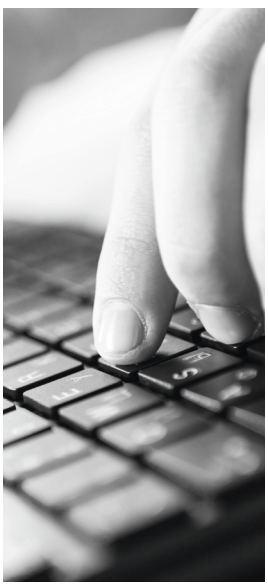
MENNESKELEG TILNÆRMING

Ein norsk lokalpolitikar kjem i snakk med ein delegasjonsmedlem 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 partiet eller i eit konkurrerande parti. Det kan vere av personleg karakter 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 datasystem for å hente ut informasjon eller ta kontroll over system. Sentralt i slike verkemiddel står ofte såkalla innsidarar. Dette er personar som har eller har hatt ein lovleg tilgang til informasjonen og systema, og som misbruker denne kunnskapen og tilgangen på ein måte som påfører andre skade eller tap. Det å lure menneske til å skaffe seg slik tilgang er noko som skjer dagleg.

Den enklaste metoden for å ta seg inn i datasystem er å få mottakarar av e-postar til å opne vedlegg eller lenkjer som startar det teknologiske angrepet. Kunnskap om til dømes sensitiv og privat informasjon eller politiske standpunkt kan utnyttast.



Kjenn verdiane dine

Vit kva som er verdifull informasjon for deg og partiet ditt

- Kva informasjon har størst verdi eller alvorlegast 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.
- Forsikre deg om identiteten til dei du kommuniserer med.
- Enkelte tema eller saker bør ikkje diskuterast på telefon eller sendast via vanleg e-post eller SMS.
- Når noko er sensitivt, bør møte bli gjennomførte 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 einina.
- Hald digitale einingar oppdaterte med siste versjon av appar/programvare.
- Bruk fleirfaktorautentisering (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 uviss 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.
- Rapporter mistenkjelege e-postar til eigen partiorganisasjon, tillitsvald for lista di eller arbeidsgivaren 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 tilgang og synlegheit etter behovet ditt.
- Ver medviten om kva du legg ut om deg sjølv og andre.
- Ver kritisk til det som kan vere falske nyheiter – unngå å spreie vidare.
- Slå av informasjon om kvar du er, om ikkje du absolutt treng å bruke det.
- Bruk eit unikt, sterkt passord og slå på fleirfaktorautentisering.

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 utsette land, bør du ikkje ta med den vanlege mobiltelefonen din, PC-en din eller nettbrettet ditt. Dette gjeld til dømes land som Noreg ikkje har eit nært tryggingspolitisk samarbeid med.

Når bør du be om rådgiving?

Ta kontakt med partiorganisasjonen din, tillitsvald eller arbeidsgivaren din om du skulle oppleve hendingar som

- mottak av e-postar som er spesielt mistenkjelege
- tekniske irregularitetar i digitalt utstyr
- tap av digitalt utstyr som mobiltelefon, PC og nettbrett
- tap av verdifull informasjon
- målretta 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.

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.

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.