



VALG

Bokmål

Du er av interesse –

Gode råd til deg som stiller til valg

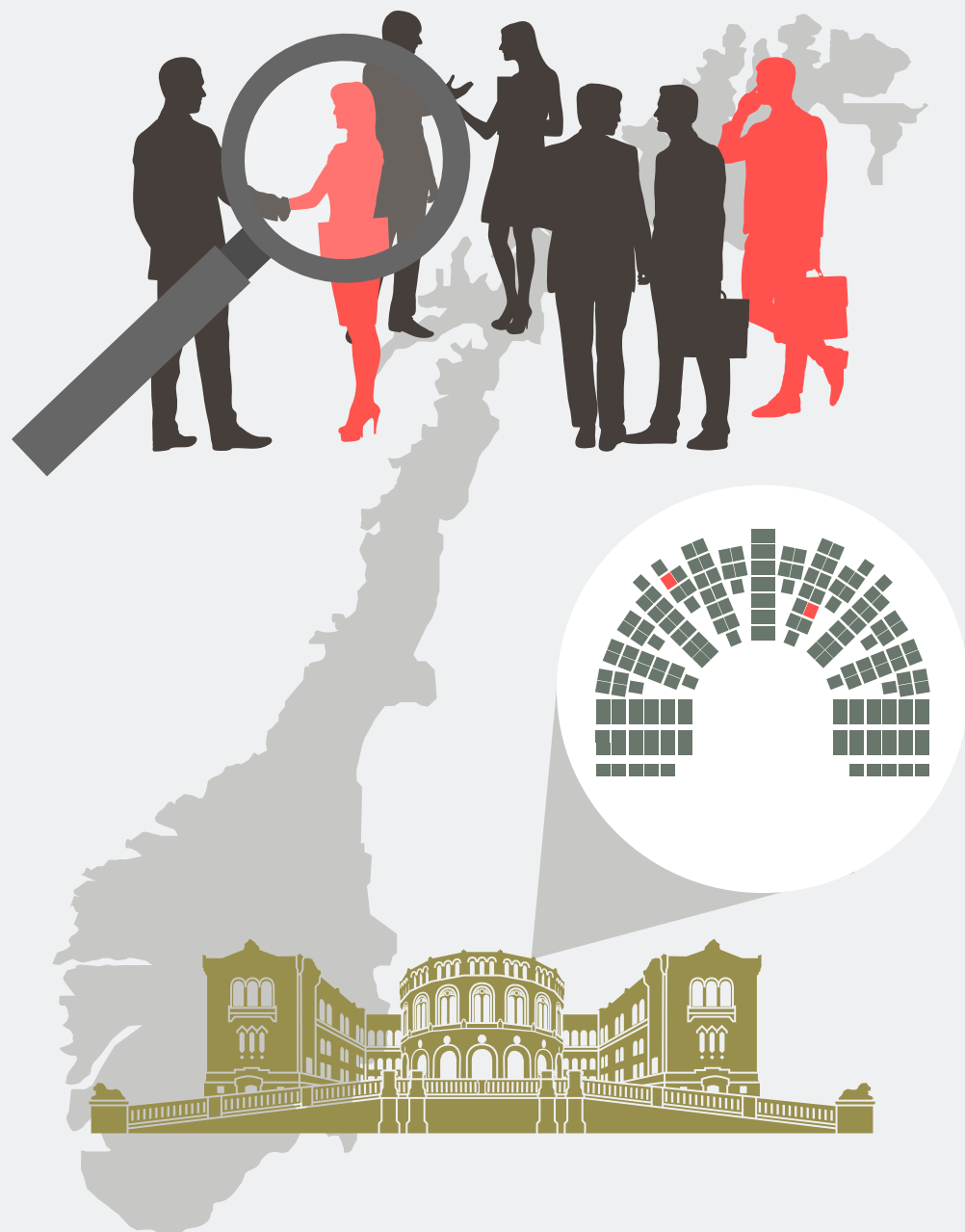


Utarbeidet av
Etterretningstjenesten,
Nasjonal
sikkerhetsmyndighet og
Politiets sikkerhetstjeneste.

Stortings- og sametingsvalget 2017

Innhold

Norge - et tillitsbasert samfunn	5
Din informasjon – ditt ansvar	5
Du er av interesse	5
Sårbarheter utnyttet	7
Kjenn dine verdier	8
Når bør du be om hjelp?	10



Norge - et tillitsbasert samfunn

Det siste året har det vært økt oppmerksomhet rundt faren for at fremmede stater aktivt søker informasjon om eller har til hensikt å påvirke politiske prosesser i andre land. Dette har bidratt til større bevissthet i befolkningen og hos politikere. Vi har et velfungerende og stabilt demokratisk system og et samfunn preget av åpenhet. Dette bidrar til robusthet både i institusjonene og hos enkeltpersoner med politiske verv. Norge har dermed et godt utgangspunkt for å stå imot eventuelle forsøk på å påvirke innenrikspolitiske prosesser. Samtidig skal vi ikke være naive. Fremmede stater vil kunne søke informasjon om norske forhold, herunder om norske individer i formelle politiske roller. Her kan hver og en av oss bidra til å sikre sensitiv informasjon om oss selv og politiske prosesser.

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 egen integritet 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

Som politiker, må du regne med at fremmede staters etterretningstjenester kan være interessert i deg. For å nå sine mål bruker de både åpne og skjulte metoder. Detaljert kunnskap om deg, både som privatperson og politiker har høy verdi. Etterretningstjenestene er dyktige til å skape relasjoner mellom mennesker, blant annet gjennom hyggelige og naturlige møter. Senere kan denne relasjonen utnyttes negativt.



FALSK E-POST

Det sendes stadig ut e-post som ugir seg for å komme fra kjente selskaper, for eksempel kan det se ut som om det sendes ut en faktura. I noen tilfeller vil det installeres skadeware på maskinen hvis du klikker på link eller åpner vedlegg, mens i andre tilfeller er de ute etter å skaffe seg informasjon om deg, for eksempel kredittkortinformasjon.



MENNESKELIG TILNÆRMING

En norsk stortingspolitiker kommer i snakk med en utenlandsk diplomat under et utenrikspolitisk seminar. Et par uker senere inviteres politikeren på lunsj av diplomaten. Lunsjen følges opp med flere møter over en lengre periode. Diplomaten ber politikeren om informasjon om andre personer i partiet. Det kan være av personlig karakter eller om fagfelt den enkelte arbeider med. Han ber også stortingspolitikeren om å legge til rette for møter med ledelsen i partiet.

Sårbarheter utnyttes

Fremmede stater forsøker kontinuerlig å ta seg inn i datasystemer for å hente ut informasjon, eller ta kontroll over systemer. Sentralt i slike virkemidler står såkalte innsidere. Med dette menes personer som allerede har en lovlig tilgang til informasjonen og systemene. Det å lure mennesker til å skaffe seg slik tilgang er noe som skjer daglig.

Den enkleste metoden for å ta seg inn i datasystemer er å få mottakere av e-poster til å åpne vedlegg eller linker som starter det teknologiske angrepet. Sensitiv og privat informasjon som er belastende og pinlig, kan brukes som utpressing.



Kjenn dine verdier



Vit hva som er sensitiv informasjon for deg og ditt parti

- ▶ Hvilken informasjon har den største verdien og den mest alvorlige konsekvensen hvis andre fikk tilgang?
- ▶ Hvem kan du dele slik informasjon med og hvem skal den ikke deles med?



Behandle sensitiv informasjon med forsiktighet

- ▶ Tenk over hva du sier og hvem som lytter – både på telefon og i det offentlige rom.
- ▶ 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 tilstede.
- ▶ Bruk krypteringsløsninger for elektronisk kommunikasjon.



Beskytt egen mobiltelefon, nettbrett og PC

- ▶ Ikke lån bort ditt elektroniske utstyr til andre.
- ▶ Hold elektronisk utstyr oppdatert med siste versjon av programvare.
- ▶ Ikke gi andre tilgang til din pc, mobiltelefon, minnepinne eller annet elektronisk utstyr.



Beskytt nettprofiler

- ▶ Bruk to-faktor autentisering (bruk av passord i kombinasjon med sms, kodebrikke eller lignende) der hvor det tilbys.
- ▶ Bruk forskjellige passord for hver tjeneste.



E-post

- ▶ Vær kritisk til linker og vedlegg i e-post som du mottar.
- ▶ Er du usikker på om du bør åpne et vedlegg eller en link - vurder om det er strengt nødvendig.
- ▶ Gjør gjerne et internettsøk på informasjonen uten å åpne linken/vedlegget.
- ▶ Rapportert mistenkelige e-poster til egen partiorganisasjon, tillitsvalgt for din liste eller arbeidsgiver.



Sosiale medier

- ▶ 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.
- ▶ Si fra til andre at du ikke ønsker at de skal tagge/merke deg på sosiale medier.



På reise

- ▶ Unngå å koble deg opp til offentlige trådløse nett. Bruk mobildata eller mobilt bredbånd.
- ▶ Dersom du reiser til utsatte land, bør du ikke ta med din vanlige mobiltelefon, PC eller nettbrett. Dette er for eksempel land som Norge ikke har sikkerhetspolitisk samarbeid med.

Når bør du be om hjelp?

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

- ▶ Mottak av e-poster som er mistenkelige
- ▶ Tekniske uregelmessigheter i digitalt utstyr
- ▶ Tap av mobiltelefon, pc og nettbrett
- ▶ Tap av sensitiv informasjon
- ▶ Misbruk av dine profiler i sosiale medier
- ▶ Spredning av falsk informasjon

Dersom du tror du er utsatt for et digitalt angrep, uønsket påvirkning eller tilnærming fra fremmede stater bør du så raskt som mulig informere og diskutere saken med din nærmeste leder. Om du fortsatt er bekymret? Ta kontakt med Politiets sikkerhetstjeneste.

post@pst.politiet.no

Tlf 23305000



MISTENKLIG EPOST

- ▶ Sjekk språket, eposter skrevet på dårlig norsk bør du være forsiktig med
- ▶ Sjekk om avsenderen er riktig. Eks: Feilstavet, slutter på .com i stedet for .no, bruker gmail eller yahoo i stedet for jobb-epost.
- ▶ Hvis du kjenner avsender, men er usikker – ring vedkommende og sjekk om de faktisk har sendt deg noe
- ▶ Er det for godt til å være sant så er det gjerne det- bruk sunn fornuft!





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