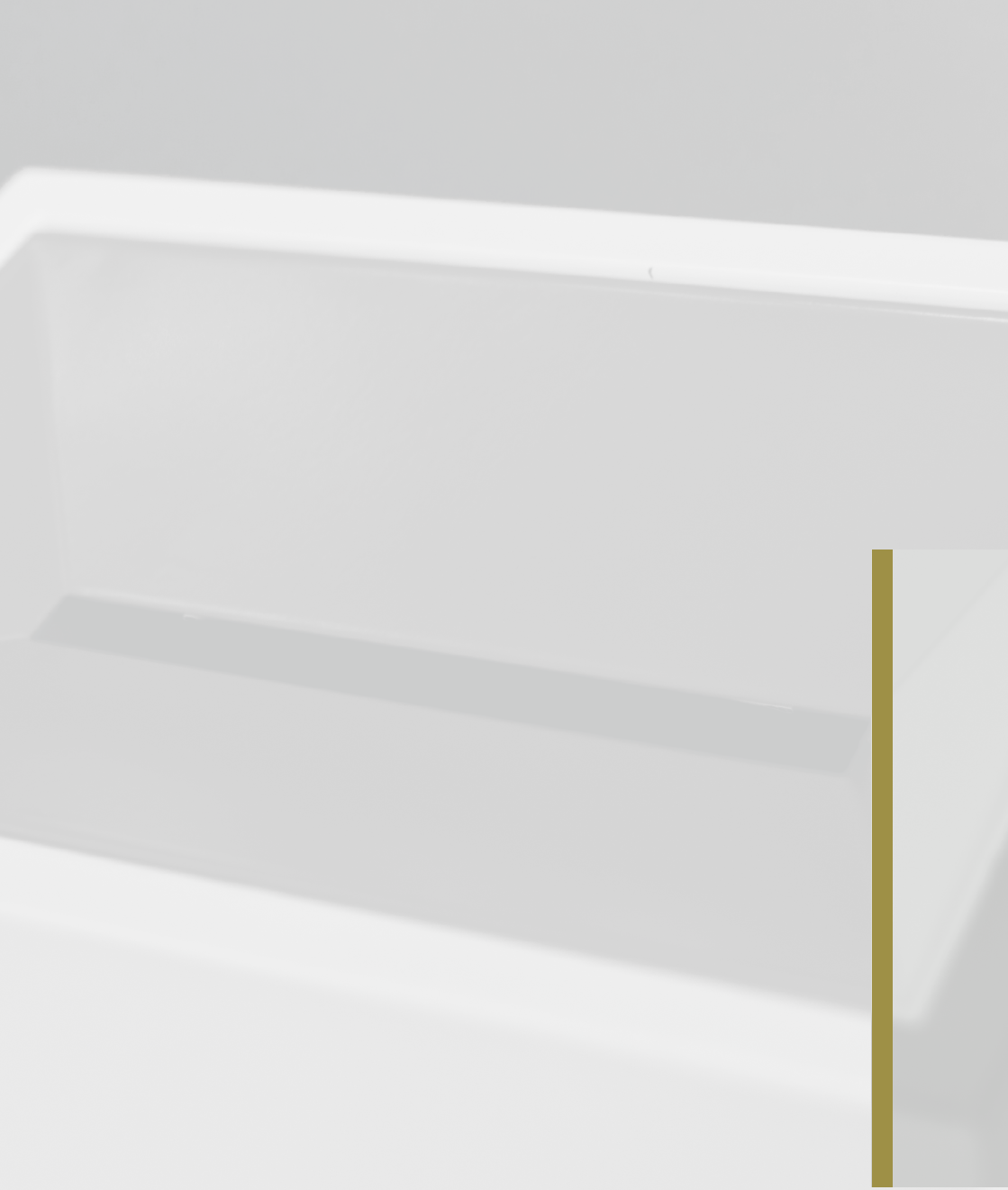
VAL

Nynorsk

Du er av interesse

Gode råd til deg som stiller til val

Utarbeidde av
Etterretningstenesta,
Nasjonalt tryggingsorgan og
Politiets tryggingsteneste.



Innhold

Noreg – eit tillitsbasert samfunn

Det siste året har det vore meir merksemd rundt faren for at framande statar prøver å påverke politiske prosessar i andre land. Vi kan definere påverknad som ein utanlandsk, statleg initiert, fordekt og tilsikta aktivitet for å oppnå eit mål som på kort eller lengre sikt kan svekkje norske interesser til fordel for ein annan stat. Slik påverknad kan vere retta mot valsystemet og gjennomføringa av valet, mot politiske aktørar eller mot veljarane og haldningane i befolkninga.

Vi har eit velfungerande og stabilt demokratisk system og eit samfunn prega av openheit. Det bidreg til at vi har robuste institusjonar, og at enkeltpersonar med politiske verv står sterkt. Noreg har dermed eit godt utgangspunkt for å stå imot forsøk på å påverke innanrikspolitiske prosessar. Samtidig skal vi ikkje vere naive. Framande statar vil kunne 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 sjølve og politiske prosessar og handtere mogleg uønskt påverknad.

Din informasjon – ditt ansvar

Du må sjølv medverke til å beskytte informasjon om deg sjølv og dei verktøya du bruker for å kommunisere. Kva du sjølv gjer, har betyding for integriteten din og evna du har til å kommunisere trygt og sikkert. Det er viktig at du har kunnskap om korleis du kan handtere situasjonar som kan innebere risiko. Det 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. Som politikar betyr det at du må rekne med at etterretningstenestene til framande statar kan vere interesserte i deg. For å nå måla sine bruker

dei både opne og skjulte metodar. Detaljert kunnskap om deg som privatperson og politikar og kunnskap om lokalpolitiske forhold kan ha

FALSK E-POST

Det blir stadig sendt ut e-postar som utgir seg for å komme frå kjende selskap. For eksempel kan det sjå ut som om det blir sendt ut ein faktura. I nokre tilfelle blir det installert skadevare på maskina dersom du klikkar på ei lenkje eller opnar eit vedlegg, mens dei i andre tilfelle er ute etter å skaffe seg informasjon om deg, for eksempel kredittkortinformasjon.

MENNESKELEG TILNÆRMING

Ein norsk politikar kjem i snakk med ein diplomat, eit 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 eit konkurrerande parti. Det kan vere av personleg karakter eller jobbrelatert. Vedkommande ber også politikaren leggje til rette for møte med leiinga i partiet eller andre interessante partar. Utanlandske aktørar som nemnde i eksemplet kan vere tilknytte eller utnytta av etterretningstenesta i landet. Dette er ein vanleg måte å operere på i Noreg.

høg verdi. Etterretningstenestene er dyktige til å skape relasjonar mellom menneske, mellom anna gjennom hyggjelege og naturlege møte. Noko så tilsynelatande banalt som kontaktlista på telefonen din kan interessere etterretningstenestene. Seinare kan denne relasjonen bli utnytta negativt.

Sårbarheiter blir utnytta

Framande statar prøver kontinuerleg å ta seg inn i datasystem for å hente ut informasjon eller ta kontroll over system. Sentralt i slike verkemiddel står såkalla insiderar. Med det meiner vi personar som allereie har ein lovleg tilgang til informasjonen og systema. 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 eit teknologisk angrep. Kunnskap om for eksempel sensitiv og privat informasjon eller politiske standpunkt kan utnyttast.

Kjenn verdiane dine

Vit kva som er sensitiv informasjon for deg og partiet ditt

- Kva informasjon har den største verdien og den mest alvorlege konsekvensen om andre fekk tilgang?
- Kven kan du dele slik informasjon med, og kven skal han ikkje delast med?

Behandle sensitiv informasjon forsiktig

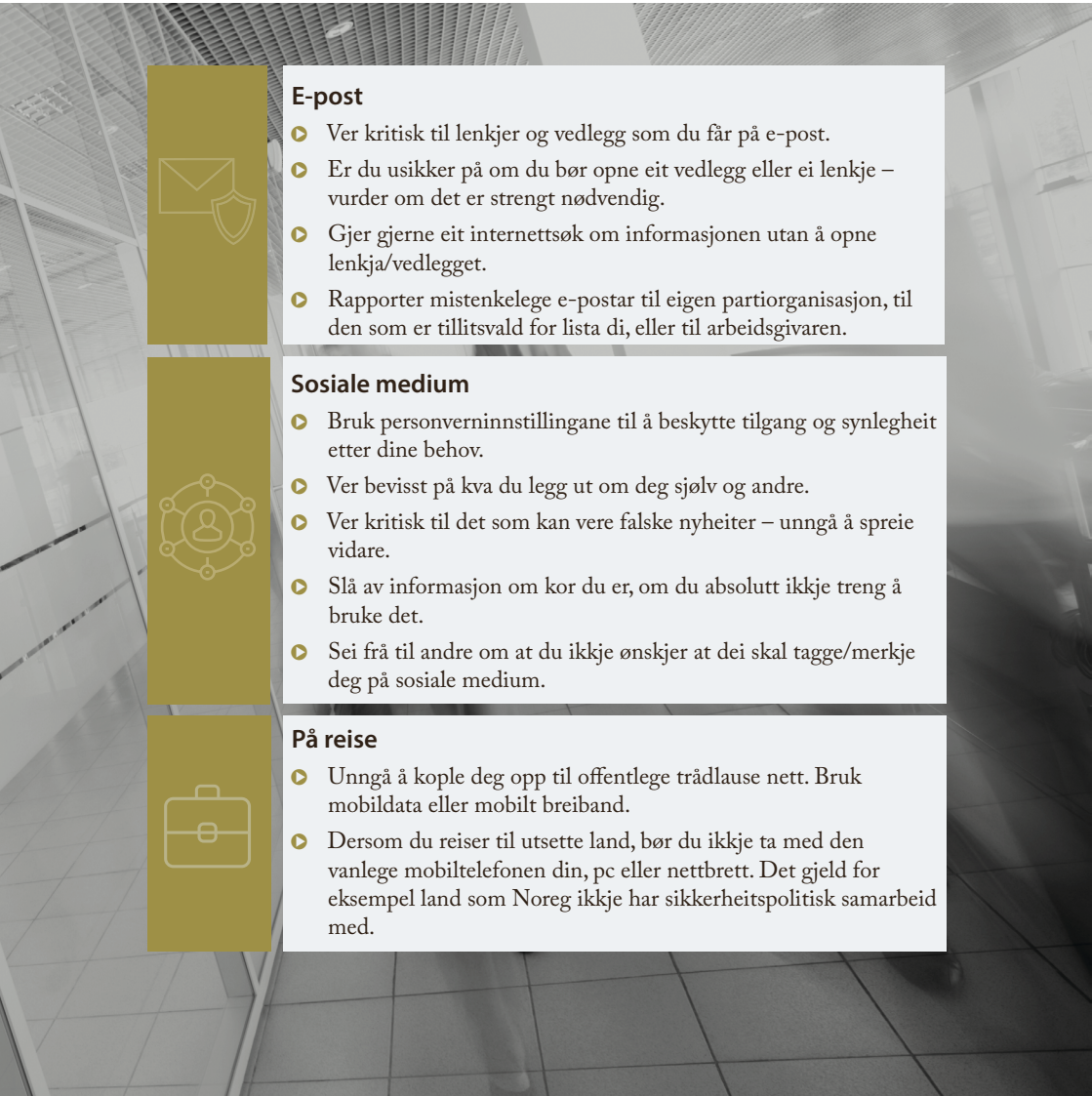
- Tenk over kva du seier, og kven som lyttar – både på telefon og i det offentlege rom.
- Enkelte tema eller saker bør ikkje diskuterast på telefon eller sendast via vanleg e-post eller SMS.
- Møte der ein tek opp sensitive saker, bør gjennomførast utan pc, mobil og smartklokker til stades.
- Bruk krypteringsløysingar for elektronisk kommunikasjon.

Beskytt eigen mobiltelefon, nettbrett og pc.

- Ikkje lån bort det elektroniske utstyret ditt til andre.
- Hald elektronisk utstyr oppdatert med den siste versjonen av programvara.
- Ikkje gi andre tilgang til pc-en, mobiltelefonen, minnepinnen eller anna elektronisk utstyr.

Vern om nettprofiler

- Bruk to-faktor autentisering (bruk av passord i kombinasjon med sms, kodebrikke eller lignande) der hvor det er mogeleg.
- Bruk ulike passord for kvar teneste.



E-post

- Ver kritisk til lenkjer og vedlegg som du får på e-post.
- Er du usikker på om du bør opne eit vedlegg eller ei lenkje – vurder om det er strengt nødvendig.
- Gjer gjerne eit internettsøk om informasjonen utan å opne lenkja/vedlegget.
- Rapporter mistenkelege e-postar til eigen partiorganisasjon, til den som er tillitsvald for lista di, eller til arbeidsgivaren.

Sosiale medium

- Bruk personverninnstillingane til å beskytte tilgang og synlegheit etter dine behov.
- Ver bevisst på 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 kor du er, om du absolutt ikkje treng å bruke det.
- Sei frå til andre om at du ikkje ønskjer at dei skal tagge/merkje deg på sosiale medium.

På reise

- Unngå å kople deg opp til offentlege trådlause nett. Bruk mobildata eller mobilt breiband.
- Dersom du reiser til utsette land, bør du ikkje ta med den vanlege mobiltelefonen din, pc eller nettbrett. Det gjeld for eksempel land som Noreg ikkje har sikkerheitspolitisk samarbeid med.

Kva tid bør du be om rådgiving?

Ta kontakt med partiorganisasjonen din, den som er tillitsvald, eller arbeidsgivaren din om du opplever

- at du får e-postar som er mistenkelege
- at det er tekniske uregelmessigheiter i det digitale utstyret ditt
- at du mistar mobiltelefon, pc eller nettbrett
- at du mistar sensitiv informasjon
- at du blir utsett for målretta tilnærming
- at nokon misbruker profilane dine i sosiale medium
- at nokon spreier falsk informasjon

Dersom du trur du er utsett for eit digitalt angrep, uønskt påverknad eller tilnærming frå framande statar, bør du så raskt som mogleg informere og diskutere saka med den nærmaste leiaren din.

Er du framleis bekymra?

Ta kontakt med relevante myndigheiter som Politiets sikkerheitsteneste (PST), Nasjonalt tryggingsorgan (NSM) eller lokalt politi.

Politi
tlf. 02800

PST:
post@pst.politiet.no
tlf. 23305000

NSM:
post@nsm.stat.no
tlf: 67 86 40 00

MISTENKELEG E-POST

- Sjekk språket – e-postar skrivne på dårleg norsk bør du vere forsiktig med.
- Sjekk om avsendaren er riktig. Det kan vere at namnet er feilstava, at adressa sluttar på .com i staden for .no, eller at avsendaren bruker gmail eller yahoo i staden for jobb-e-post.
- Dersom du kjenner avsendaren, men er usikker – ring vedkommande og sjekk om han eller ho faktisk har sendt deg noko.
- Er det for godt til å vere sant, så er det gjerne det. Bruk sunn fornuft!

Denne brosjyra er laga av Etterretningstenesta, Nasjonalt tryggingsorgan og Politiets tryggingsteneste på oppdrag fra Forsvarsdepartementet og Justis- og beredskapsdepartementet, koordinert med Kommunal- og moderniseringsdepartementet og Valdirektoratet.