Personlig sikkerhet

En veileder for myndighetspersoner og andre risikoutsatte

PST
POLITIETS SIKKERHETSTJENESTE

1. utgave 2024

Politiets sikkerhetstjeneste (PST) håndterer de alvorligste truslene mot landets sikkerhet og demokratiet vårt.

Skann koden for den digitale utgaven av sikkerhets-håndboken.

Du finner den også på pst.no

Innhold

Side

1 Sikkerhet er et felles ansvar

PST har et særskilt ansvar for å forebygge og etterforske trusler mot landets myndighetspersoner. Samtidig ligger det også et ansvar for forsvarlig sikkerhet på den enkelte og deres virksomhet eller parti/organisasjon. Det er grunnleggende for demokratiet at våre myndighetspersoner kan utføre sine oppgaver på en trygg og sikker måte. Denne håndboken skal bidra til dette.

Myndighetspersoner innbefatter medlemmer av Kongehuset, Stortinget, regjeringen og Høyesterett. PST har i tillegg ansvar for å etterforske straffbare handlinger som er begått mot sentralstyremedlemmene i ungdomspartiene dersom disse har sin bakgrunn i deres politiske virke.

I denne sikkerhetshåndboken samles informasjon og veiledning med formål om å øke sikkerhetsbevisstheten og tryggheten for myndighetspersoner. Håndboken er delt inn etter utvalgte sentrale temaer som gjelder arenaer der du som myndighetsperson kan være trussel- og risikoutsatt. Hvert tema har tilhørende råd om forebyggende sikkerhetstiltak og/eller handlingsmønster som kan redusere konsekvensene hvis uønskede hendelser likevel skulle oppstå.

Sikkerhetshåndboken er først og fremst skrevet for myndighetspersoner. Rådene som blir gitt, har imidlertid også overføringsverdi til andre offentlige personer, politisk aktive, samt yrkesgrupper og personer som av ulike årsaker er risikoutsatt.

Råd for fysisk sikkerhet

Råd om fysisk sikkerhet vil avhenge av situasjonen du befinner deg i. Det er i utgangspunktet trygt å være politiker i Norge. Sikkerhetsrådene kan regnes som forholdsregler på samme måte som at vi er årvåkne i trafikken og bruker bilbelte. I et demokrati er det viktig for folkevalgte å være tilgjengelige for velgerne. Rådene skal ikke være til hinder for politisk virksomhet og egne behov, men styrke dine forutsetninger for å vurdere risiko og redusere denne til et akseptabelt nivå. Både på vegne av deg selv og for din funksjon som en del av landets øverste myndigheter.

Trusselvurderinger og ulike sikkerhetstiltak for deg som myndighetsperson skal ikke kommenteres i media eller på annen måte gjøres tilgjengelig for offentligheten.

Eksempel på risikohåndtering i hverdagen

Er du trusselutsatt, eller forventer du å bli det?
Det kan være grunn til å være ekstra sikkerhetsbevisst hvis du, (parti)organisasjonen eller virksomheten skal til et sted eller arrangement der du kan være mer utsatt enn normalt, eller til et land der det er forhøyet trusselnivå.

Uønskede hendelser kan oppstå når

- du/dere er involvert i kontroversielle saker med stor medieoppmerksomhet og der sterke følelser er i sving
- det er et stort personfokus på deg eller (parti)organisasjonen/virksomheten
- det kan forventes forstyrrelser fra aktivister eller andre

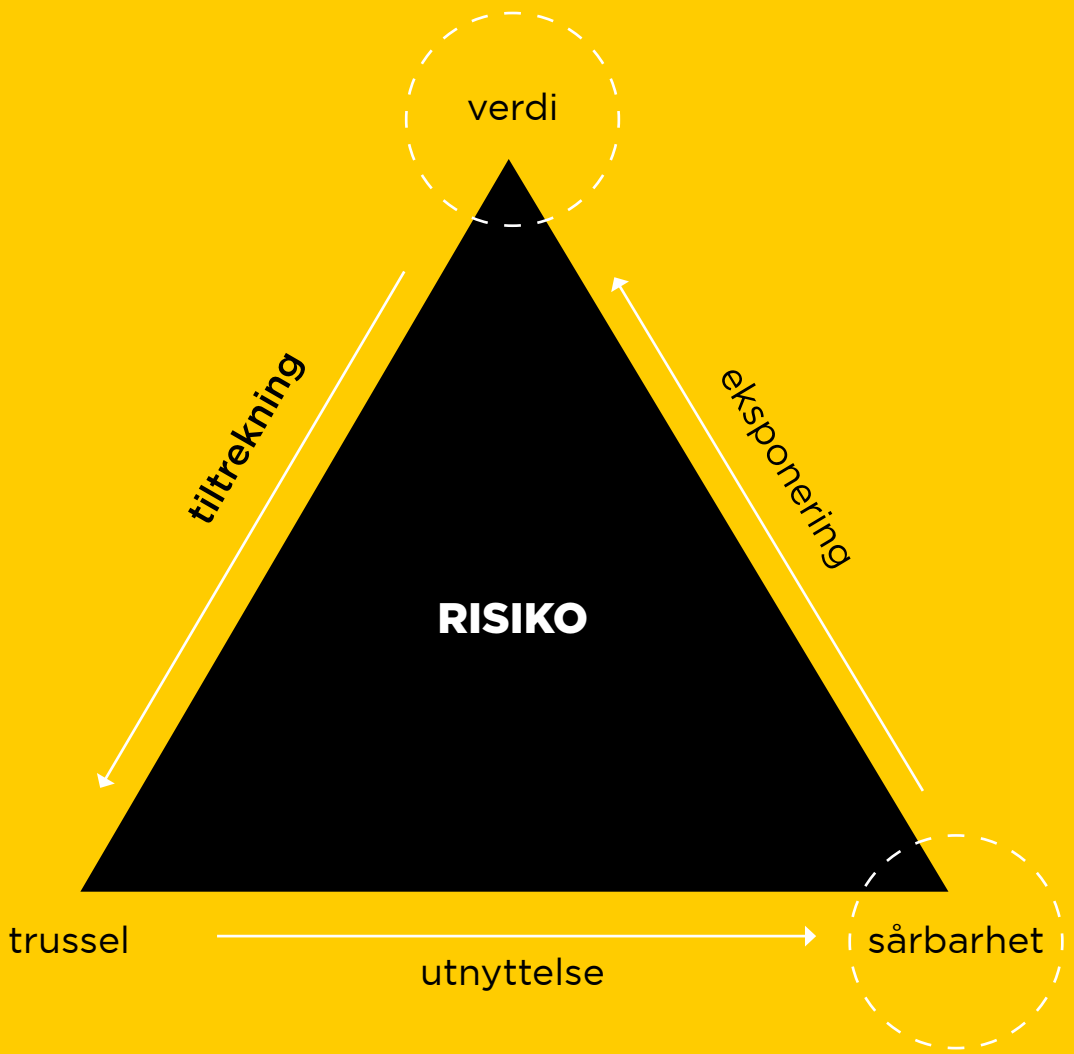
Hvilke tiltak kan du iverksette?

- Gjør små risikovurderinger i hverdagen. Vær bevisst på når, hvor og hvordan du er sårbar for ulike trusselaktører. Iverksett hensiktsmessige sikkerhetstiltak ved behov.
- Vær mentalt forberedt sikkerhetstruende hendelser.
- Snakk med personer i egen (parti)organisasjon/virksomhet, sikkerhetsansvarlige eller PST/politiet om du er usikker eller trenger råd.
- Håndter sensitiv informasjon slik at den ikke blir tilgjengelig for andre.
- Varsle dersom du utsettes for trusler eller trusselrelevante hendelser.

1.1 | Risikoforståelse

Det finnes ulike måter å beskrive risiko på. I denne håndboken ser vi på risiko som en kombinasjon av verdi, trussel og sårbarhet. I hverdagen vurderer vi alle mer eller mindre bevisst risiko. For en myndighetsperson er mer rutinemessige og strukturerte risikovurderinger viktig som en følge av posisjonen man har.

Forståelse av egne verdier og en grunnleggende kjennskap til det rådende trusselbildet er viktig. Vurderingene skal belyse i hvilken grad man er sårbar, og om det bør iverksettes sikkerhetstiltak. Vurderingsprosessen i seg selv, og også enkle tiltak, vil ha betydelig positiv innvirkning på risikoen totalt sett.



2 Personsikkerhet
(trygghet i hverdagen)

Sannsynligheten for truende hendelser, og dermed behovet for sikkerhetstiltak, vil kunne variere både i tid og fra person til person. Behovet for konkrete sikkerhetstiltak vil også avhenge av hvilken posisjon du har. PST anbefaler alle myndighetspersoner å være sikkerhetsbevisste både på jobb og i fritiden. Truende hendelser kan gjøre alvorlig skade både for den som utsettes for det, for familie og andre nærstående og for samfunnet for øvrig.

Ulike aktiviteter og situasjoner, som politisk virksomhet og offentlige og/eller forhåndsannonserte møter, kan medføre økt sannsynlighet for at uønskede hendelser inntreffer. Det er derfor viktig å ha en sikkerhetsbevisst adferd som både forebygger uønskede hendelser, og som gjør at man håndterer dem best mulig hvis de skulle oppstå. Snakk gjerne sammen om hvilke ulike uønskede hendelser som kan inntreffe, og diskuter hvordan de bør håndteres, og hvem man varsler. Det er viktig å gjøre seg kjent med sikkerhetsrutiner på jobb, hjemme, på arrangementer og ellers ute i samfunnet.

Eksempler på scenarioer som kan inntreffe i hverdagen

- Noen kommer opp i ansiktet på deg, kjefter og er så nærgående at du blir dyttet om du ikke trekker tilbake.
- Noen lager bråk ved valgboden og kaster brosjyrer rundt seg.
- Noen kjenner deg igjen på gaten og begynner å følge etter deg.
- Det står plutselig en fremmed person i hagen din eller på verandaen din.
- En fremmed ringer på døren din og insisterer på at du skal åpne.

2.1 | Familie

Trusler mot deg som myndighetsperson vil også kunne ramme eller påvirke familien. Alle familiemedlemmer bør derfor være oppmerksomme på mulige trusselsituasjoner og hvordan man kan være sårbar for slike hendelser, og ha kjennskap til hensiktsmessige sikkerhetsråd. God sikkerhet bygges i fellesskap.

Snakk om sikkerhet

- Når din posisjon eller konkrete forhold medfører en større mulighet for trusselhendelser, kan det være hensiktsmessig at du informerer dem rundt deg.
- Trusselinformasjon eller sikkerhetsfokus kan medføre unødig utrygghet. Tenk på sikkerhetstiltak som naturlige, men viktige forholdsregler, for eksempel på samme måte som man forbereder seg på dårlig vær når man ferdes i fjellet.
- Personell i barnehage, på skole og på fritidsaktiviteter bør informeres og oppdateres om nye rutiner.
  - De som henter barn, bør ikke være ukjente for personellet.
  - Man er mer sårbar alene. Legg til rette for at barn kan gå sammen med en venn eller en voksen til og fra skole og fritidsaktiviteter.
- Legg til rette for at dine nærmeste informerer deg om uvanlige hendelser og deler eventuelle bekymringer.

2.2 | Vær sikkerhetsbevisst ved opptreden på offentlig sted

Støtteapparatet rundt myndighetspersoner kan aktivt bidra til å øke sikkerheten under planlagte møter med publikum. God dialog med arrangøren og andre involverte aktører er viktig både for felles sikkerhetsbevissthet, for å innhente relevant informasjon og for tilrettelegging av enkle sikkerhetstiltak.

Vurderinger ved offentlig tilgjengelige arrangementer

- Hvem er arrangør og eventuell ansvarlig for sikkerheten på stedet?
- Er det en fare for sikkerhetstruende hendelser, og foreligger det en handlingsplan dersom noe skulle skje? Hvordan kan slike hendelser forebygges, og hva gjør arrangøren om noe skulle skje?
- Vil det være vakter til stede?
- Er det andre deltakere til stede som kan oppfattes som kontroversielle eller tiltrekke seg uønskede personer? Er stedet og området belastet på noen måte?
- Vil det være adgangskontroll?
- Er det andre myndighetspersoner til stede?
- Er området rundt scenen avgrenset eller avsperret?
- Er det behov for å varsle PST eller politiet i forkant av arrangementet? Det kan være at myndighetene har relevant informasjon eller vil vurdere egne tiltak.
- Hva skal man forhåndsannonsere? Ankomsttid, sted for ankomst, hvordan man som myndighetspersonen ankommer, eller hvor man oppholder seg før og etter arrangementet, er opplysninger en potensiell trusselaktør kan utnytte, og som derfor bør skjermes.
- I særlige tilfeller bør man vurdere å vente med å offentliggjøre en myndighetspersons deltakelse til etter at et møte eller arrangement er gjennomført.

Generelle sikkerhetsråd for opptreden i det offentlige rom

Nærhet til publikum

- Forsøk å skape en terskel eller avstand mellom deg selv og publikum, eksempelvis en talerstol, et bord eller bånd og lignende. Slike terskler virker forebyggende, og det kan fungere som et varsel dersom de krysses.
- Hvis noen vil overrekke en gave, bør det vurderes om den bør mottas av andre, og om den bør pakkes opp av giveren selv.

Ha oversikt og ryggen fri

- Myndighetspersoner og andre profilerte politikere bør unngå å havne midt i en folkegruppe med få eller ingen retrettmuligheter.
- Ukjente eller uvedkommende bør ikke ha tilgang til nærområdet bak deg.
- Gitt en truende eller annen uønsket hendelse er det en fordel om du kan forlate stedet uten å måtte gå gjennom publikum.

Vær forberedt på forstyrrelser

- Ha alltid med mobil og alarm (hvis du har det). Tenk gjennom tiltak og rollefordelinger på forhånd.
- Hvis noen er forstyrrende eller opptrer truende, er det best å prøve å unngå å provosere vedkommende. Trekk deg heller unna til situasjonen er håndtert.
- Gjør deg kjent med planlagt vei inn og ut av et møtested samt alternative rømningsveier slik at du raskt kan forlate en farlig eller uønsket situasjon for å komme deg i sikkerhet.

Sett grenser for hva som er akseptabelt, både fysisk og på internett

- Grenser er individuelle barrierer for hva man aksepterer i kontakt med andre. Praktiser grensesetting i både det fysiske og det digitale rom.
- Øv deg på å avslutte uønskede samtaler på en høflig, men bestemt måte og på et tidlig tidspunkt. Dette kan forebygge situasjoner som kan utvikle seg til hets, hatefulle ytringer og trusler. Det er ofte ikke noe poeng i å «redde situasjonen» om det bygges opp til farlige eller andre uønskede omstendigheter.

Opptre sammen

- Potensielle trusselaktører kan ha en høyere terskel for å konfrontere noen hvis dere er flere.
- Det gir også mulighet for å støtte og avlaste den som blir konfrontert eller utsatt for annen uønsket adferd, og å varsle andre om situasjonen som har oppstått.

Bruk av bil gjør deg mindre sårbar

- Benytt bil som fremkomstmiddel.
- Utsatte myndighetspersoner bør begrense bruk av kollektivtransport i bysentrum. På buss, trikk eller tog er man statisk og dermed mer sårbar, dessuten blir muligheten for å trekke seg unna betydelig redusert.
- Et kjøretøy kan være et trygt sted å trekke seg tilbake til dersom uønskede hendelser skulle oppstå.

Bruk av drosje

- Bruk av drosje er også et godt forebyggende sikkerhetstiltak.
- Drosje eller tilsvarende transporttjenester bør helst bestilles på forhånd. Noter deg informasjon om bilen som er bestilt.
- Vent med å gå ut til drosjen til den har kommet.

2.3 | Forebyggende sikkerhetstiltak for egen bolig

Ditt eget hjem er et sted der du oppholder deg mye, og der du skal føle deg trygg. Samtidig er det mange som vet, eller som kan finne ut, hvor du bor. Egen bolig er derfor et sted der potensielle trusselaktører kan oppsøke deg.

Det er flere sikkerhetstiltak som kan iverksettes i en bolig. For mange holder det med enkle tiltak, for andre er det behov for mer inngripende sikkerhetsforanstaltninger. Gjør deg kjent med boligen din, hvilke sårbarheter den har, og om sårbarhetsreduserende tiltak bør utføres. Avhengig av situasjonen din kan du som myndighetsperson få råd om sikring av bolig fra vaktselskap, politiet eller PST.

Skallsikring, dører og vinduer

- Har du brevluke i ytterdøren, anbefales det at denne stenges, eventuelt at du har en brannsikker kasse på innsiden av brevluken.
- Vær bevisst på om vinduer og dører er åpne. Lukk eller lås dem når ingen er hjemme. Husk at et vindu som er «låst i åpen posisjon», kan forseres og vil kunne medføre økt sårbarhet. Vinduer og dører nær bakkeplan bør ha samme sikkerhetsnivå som ytterdøren.
- Benytt sikkerhetslås på døren ved behov, og monter kikkhull. Se og verifiser alltid hvem som er på den andre siden, før du åpner døren.
- Gjør deg kjent med beskyttelsesnivået på dører og vinduer. Disse kan beskyttes ytterligere med spesialfolie eller gitter. Det kan gi en bedre beskyttelse mot inntrengning.

Nøkler, kort og koder

- Ha kontroll på nøkler, adgangskort og portnøkler og sørg for at disse ikke kan identifiseres hvis de kommer på avveie. Bytt adgangskoder jevnlig, og vask kodeflater, da det er mulig å finne ut hvilke tall som inngår i kombinasjonene for ulike tastaturer og displayer.

Boligalarm

- Vurder å installere boligalarm. Gjør deg kjent med alarmsystemet.
- Det kan være en fordel å ha kameraovervåkning og/eller lyskastere som utløses av bevegelsessensorer, utenfor boligen.

Trygge rom

- Identifiser det tryggeste rommet i boligen. For eksempel et rom som er mulig å låse, og som ikke har vindu. Sjekk at du har mobildekning i dette rommet eller har andre måter å kommunisere ut derfra på.

Egen bolig er et sted der potensielle trusselaktører kan oppsøke deg.

Anonymiser boligen

- Unngå å ha navn på ringeklokke, dør og postkasse.
- Unngå å legge ut detaljer fra boligen på nett med informasjon som kan utnyttes av en potensiell trusselaktør. Det samme gjelder intervjuer som kan bidra til å identifisere hvor du bor, eller området du bor i.

Innsyn

- Vær bevisst på hvor det eventuelt er innsyn, både ute og inne.
- Bruk eventuelt gardiner, persienner eller annen skjerming. Det er spesielt viktig når det er mørkt ute. Hekk, mur, levegger og gjerder rundt uteområder kan ha god skjermingseffekt.
- Sittegrupper og lignende bør plasseres hensiktsmessig med tanke på både skjerming og mulighet for raskt å kunne trekke inn i boligen ved behov.

Grenser og barrierer

- Ha tydelige grenser som gjerde eller hekk rundt egen eiendom. Eventuell port/ytterdør bør holdes lukket og låst. Be gjerne naboer om å si fra hvis de ser noe som avviker fra normalen.

Skjerming av kjøretøy

- Om mulig, parker bilen i egen garasje, ute av syne på egen eiendom og slik at registreringsnummeret ikke er synlig fra offentlig sted. Unngå fast gateparkering.

2.4 | Tradisjonelle og sosiale medier

For den som er politisk aktiv, er det viktig å nå ut til store og ulike målgrupper, blant annet gjennom deltakelse i tradisjonelle og sosiale medier. Sosiale medier følges av enkeltpersoner og mediene, og det er stor interesse for politikeres digitale tilstedeværelse. Imidlertid kan eksponering i ulike medier føre til uønskede sårbarheter for deg personlig og for ditt eller andre aktørers virke. Opplysninger om familie, venner, hvem du omgås, samt faste rutinepregede aktiviteter kan utnyttes til kartlegging av deg. Privat og annen sensitiv informasjon kan misbrukes og i verste fall benyttes til å underbygge eller forsterke trusler, samt anvendes i utpressingsøyemed. Det samme kan gjelde informasjon om virksomheter og steder du besøker.

Du kan lese mer om informasjonssikkerhet i kapittel 4.

Veileder for sosiale medier

Vær kritisk

- Profiler i sosiale medier kan være falske. Også informasjon i sosiale medier kan være falsk.
- Henvendelser og lenker du mottar i ulike sosiale medier og meldingsapper, kan være avanserte forsøk på cyberangrep.
- Gjør en kritisk vurdering før du installerer apper, og ha restriktive personverninnstillinger i alle sosiale medier og apper.

Begrens eksponering av oppholdssteder og vaner

- Skill mellom offentlige og private profiler, og hold disse adskilt.
- Det er greit å være personlig, men ikke vær privat. Unngå å tilgjengeliggjøre privat informasjon som bilder av egne barn og egen bolig. Slik informasjon kan komme på avveie og utnyttes.
- Ikke legg ut informasjon om hvor du og dine nærmeste oppholder dere privat. For eksempel hvor du pleier å trene og handle, hvor barna går i barnehage / på skole, hvor du skal på ferie, eller andre steder du besøker regelmessig.
- Det kan være hensiktsmessig å vente med å legge ut informasjon om hvor du oppholder deg i jobbsammenheng, til aktiviteten er over.
- Familiemedlemmer eller andres aktivitet i sosiale medier kan eksponere det du selv ønsker å skjerme. Ta samtalen om dette med dem som står deg nær.

Eksponering i ulike medier kan føre til uønskede sårbarheter.

Kontroller og moderer

- Dersom du har en offisiell side i sosiale medier, bør det etableres klare retningslinjer for hvordan trusler og hatefylte ytringer skal håndteres. Det kan være hensiktsmessig at sosiale medier administreres av noen i ditt støtteapparat.
- Dersom du opplever ytringer i sosiale medier som påvirker deg negativt, er det viktig at du tar dette opp med andre. Be om støtte og råd fra (parti)organisasjonen eller virksomheten.

Varsle

Ta kontakt med din (parti)organisasjon eller virksomhet dersom du opplever hendelser som

- mottak av e-poster eller meldinger som er mistenkelige eller uvanlige
- misbruk av profiler i sosiale medier
- spredning av falsk informasjon

Ved potensielt straffbare ytringer, for eksempel trusler:

- Ta skjermdump eller bilde av innlegget og profilen som publiserte det. Få med kontekstuell informasjon og meld fra både til egen (parti)organisasjon/virksomhet og til PST eller politiet.

Du finner mer informasjon blant annet på
Norsis: Sosiale medier og Nettvett: Veiledninger.

2.5 | Håndtering av fysiske trusler og angrep

I Norge har det generelle trusselbildet mot myndighetspersoner vært stabilt over en lengre periode.[1] Som myndighetsperson bør du likevel være forberedt på at en uønsket eller truende hendelse kan inntreffe. Det er derfor fornuftig at du på forhånd ser for deg ulike alvorlige scenarioer som kan oppstå, og forbereder deg og dem rundt deg på hvordan du/dere kan handle i slike kritiske situasjoner. En slik mental forberedelse kan i noen tilfeller være avgjørende for å redusere konsekvensene av et forsøk på eller en gjennomført alvorlig voldshandling. Du bør se for deg og forberede deg på scenarioer som kan oppstå i forbindelse med ulike situasjoner, for eksempel under en offentlig opptreden, på internett, på arbeidsplassen eller i tilknytning til hjemmet.

1) Se PSTs oppdaterte *Nasjonal trusselvurdering* om trusselbildet for myndighetspersoner.

Håndtering av trusler eller akutte situasjoner

Vær forberedt

- Tenk gjennom mulige scenarioer på forhånd. Sett en klar grense for hva som aksepteres. Personlig fremmøte og direkte kontakt utenfor profesjonelle rammer, for eksempel på fritiden eller hjemme hos deg, bør ikke tolereres.
- Sjikanerende eller truende personer bør bortvises eller avvises.

Dersom du opplever å bli truet

- Føler du deg truet, skal du varsle! Ikke vent med å få en mulig truende situasjon bekreftet.
- Prøv å opptre rolig.
- Hør etter hva vedkommende sier. Forsøk å notere ned info om kjønn, alder, navn, dialekt, bakgrunnsstøy, telefonnummer, hva vedkommende er opptatt av, hva som er planen videre, motiv osv. Ta opp samtalen om mulig.
- Kontroller avslutningen av samtalen. Gi beskjed om hvorfor samtalen avsluttes, for eksempel at vedkommende oppleves som truende. Vær tydelig på at fremtidige henvendelser vil bli avvist og rapportert.

Ved bopel/fritidsbolig

- Trekk inn i boligen og lås døren.
- Gå til sikkert rom.
- Utløs alarm eller varsle politiet på 112.

På offentlig sted

Si fra om noen tråkker over grensene dine (for eksempel «dette er truende – hold avstand!»).

Hvis dette ikke er tilstrekkelig:

- Unngå konfrontasjon og trekk deg unna.
- Oppsøk et sted med andre personer. Tilkall oppmerksomhet og hjelp.
- Utløs alarm eller varsle politiet på 112.
- Gjør motstand hvis du må.

2.6 | Terrorangrep og andre alvorlige voldsscenarioer

Selv om det er lav sannsynlighet for at du blir utsatt for et terrorangrep, kan kunnskap om slike og innsikt i hvordan du bør opptre, redde livet ditt. Dette er uavhengig av om det skjer i Norge eller i utlandet. En måte å være mentalt forberedt på er å forestille seg ulike scenarioer og situasjoner samt ulike måter å handle på. Det vil være kort tid fra du forstår hva som har skjedd, til du må handle for å komme deg ut av situasjonen. Ved en forhøyet terrortrussel bør du være bevisst på særlig trusselutsatte områder. Det kan være ved sikkerhetskontroller, ved inngangspartier eller utenfor potensielle mål. Gjør deg kjent med rømningsveier og nødutganger på hoteller, i bygninger og på offentlige steder.

Handling ved terrorangrep og andre alvorlige voldsscenarioer

Dersom du ledsages av sikkerhetspersonell, må du følge deres råd og ordrer.
Dersom du er alene, gjelder følgende ved et terrorangrep:

1. Flykt

- Vurder, ta initiativ og handle.
- Kom deg bort fra området. Ikke ta med deg noe unødvendig, og hold hendene synlig. Advar andre.
- Dersom terrorangrepet startet med en eksplosjon, må du være oppmerksom på andre farer, som branner, gasslekkasjer og ødelagte bygninger.
- Vær forberedt på at ytterligere angrep kan inntreffe, for eksempel fra bevæpnede terrorister.

2. Søk dekning

- Dersom det ikke er mulig å rømme, eller du er i nærheten av gjerningspersonene, finn et sikkert gjemmested som kan låses eller barrikaderes.
- Lås, slukk lyset og vær stille. Hold deg unna vinduer og dører til faren er over.
- Skru av all lyd og vibrering på mobilen, og skru ned lysstyrken på skjermen for ikke å avsløre hvor du er.
- Ikke ring unødvendig til personer som kan befinne seg i området. Det kan utsette dem for fare.
- Ikke forlat gjemmestedet før politiet har gitt klarsignal.
- Skjul og dekning er ikke alltid det samme: Husk at selv om en terrorist ikke kan se deg, kan du likevel bli rammet av skudd.
- Dersom du ikke har annet valg og det står om livet, angrip gjerningspersonen med alle tenkelige hjelpemidler.

3. Varsle

- Varsle politiet så raskt som mulig, alternativt send melding til noen som kan ringe for deg. Du kan ha viktig informasjon som gir politiet forutsetninger for å stanse angrepet.
- I en alvorlig situasjon kan telenettet overbelastes. Det kan være vanskelig å ringe politiet. I slike tilfeller kan meldinger ofte fortsatt brukes. Noen apper gir stedslokasjon til nødetatene.
- Kan du ikke snakke, kan du ha en åpen linje på telefonen slik at politiet kan lytte til hva som skjer.
- Følg politiets anvisninger. Når politiet kommer til stedet, er det viktig at du opptrer rolig og ikke på en måte som kan oppfattes som at du kan være gjerningsperson. Ikke ha noe i hendene og hold dem synlig for politiet. Forhold deg rolig, og vær forberedt på at du kan bli pekt på med skytevåpen.

2.7 | Rapporter alle trusler til myndighetene

Trakassering, trusler og vold kan inntreffe til tross for forebyggende tiltak. Det er viktig at alvorlige og straffbare trusler rapporteres til myndighetene. Selv om du er usikker, bør du likevel ta kontakt med PST eller politiet for at de kan gjøre en vurdering. Informer også internt i virksomheten eller (parti)organisasjonen samt nærmeste leder. Det bør tas en skjermdump av ytringer og trusler, eventuelt bør disse lagres, slik at de blir tilgjengelige for politiet eller PST i forbindelse med deres undersøkelser og eventuelle etterforskning.

Avhengig av hvem trusselen er rettet mot, og motivet bak trusselen er det enten PST eller politiet som etterforsker slike saker. Dersom det fremsettes en trussel mot en myndighetsperson og trusselen kan knyttes til vedkommendes rolle og posisjon, er det i utgangspunktet PST som har ansvaret for å etterforske saken. PST og politiet kan vurdere å øke sikkerhetstiltak på bakgrunn av mottatte trusler, uavhengig av om saken etterforskes. Det er derfor viktig å varsle: heller en gang for mye enn en gang for lite. Se PSTs veileder «Mottaksvurdering for bekymringsfulle hendelser» på siste side av håndboken.

Varsling om trusler

- Hvis det er fare for liv og helse, utløs alarm eller ring politiets nødnummer **112**.
- Ved andre straffbare forhold eller bekymringer, ring **02800**, som går til lokalt politiet der du er.
- Trusler mot myndighetspersoner (som ikke er akutte) varsles i etablerte kanaler eller til PSTs døgnåpne responssenter:
  23 30 50 00 / post@pst.politiet.no
- Det er også mulig å sende en e-post til både PST og politiet selv om det ikke foreligger en konkret trussel. Potensielt sikkerhetstruende forhold kan være sammensatte og utvikle seg over tid. Kunnskap om slike forhold er relevant for PST og politiet, som grunnlag for både konkrete sikkerhetsvurderinger og tiltak, og opprettelse av straffesaker.

3 Sjikane, hets og trusler

Konkrete trusler, men også et stort omfang av fiendtlige og negative personrettede ytringer, har store negative konsekvenser for mange myndighetspersoner og deres nærmeste. Det stadig økende omfanget av hets, sjikane og trusler mot politikere kan føre til at enkelte velger å trekke seg fra den offentlige debatten, modererer seg eller avstår fra å stille til valg og videre politisk arbeid. Norsk forskning viser at halvparten av lokalpolitikere som har mottatt trusler, ikke snakker om det med andre, og bare en av ti rapporterer det til politiet. Sjikane, hets og trusler er en alvorlig utfordring for demokratiet.

Hets, sjikane og trusler fremsettes hovedsakelig i kommentarfelt og i sosiale medier på internett. De som står bak denne aktiviteten, er ofte drevet av en personlig motivasjon og/eller er i en vanskelig livssituasjon. En fellesnevner for disse personene er at de er myndighetsfiendtlige. Ytringene knyttes ofte til politiske enkeltsaker, partitilhørighet eller generell «trolling». De fleste retter ytringen sin mot rollen din og partiet du representerer, og i mindre grad mot deg som person. De færreste som fremsetter trusler, har en reell voldsintensjon, og svært få som har blitt utsatt for slike ytringer, har opplevd fysiske angrep eller forsøk på det.

Enkle tiltak kan redusere sannsynligheten for at du mottar denne typen uønskede ytringer. Ofte består slike tiltak i å redusere og begrense den direkte tilgangen til deg og dine nærmeste, ikke minst i sosiale medier og på internett for øvrig.

Myndighetspersoner og politikere må likevel være forberedt på et tøft og ubehagelig personfokus og debattklima. Et viktig mål med forebyggende sikkerhetstiltak er å redusere den negative virkningen som sjikane, hets og trusler kan få for de mange som utsettes for dette. Den som opplever trusler, opplever ofte utrygghet ved å stå alene og selv være ansvarlig for å håndtere uønskede hendelser og konsekvenser av disse. Det er derfor viktig at (parti)organisasjonen eller virksomheten står samlet rundt dem som utsettes for hets, sjikane og trusler. Gode rammer, rutiner og tiltaksplaner gjør deg som myndighetsperson mer robust.

Rådene må ses i sammenheng med kapittel 2: *Personsikkerhet,* og kapittel 4: *Informasjonssikkerhet.*

Forebyggende råd

Gjør deg kjent med innholdet i veilederen Hatogtrusler.no

- Hatogtrusler.no gir informasjon og veiledning for politikere som opplever hets, hatefulle ytringer og trusler. Den inneholder referanser til forskning, rådgivning osv.

Skjerm deg fra unødvendig informasjon

- Forum og kommentarfelt kan ofte inneholde personrettet sjikane eller trusler. Monitorering av slike arenaer kan over tid være belastende. I den grad det er nødvendig, kan det være hensiktsmessig at andre følger opp sosiale medier på vegne av deg.

Sett grenser

- Sjikane og trusler skal ikke tolereres. Avslutt samtaler eller diskusjoner som utvikler seg i en slik negativ retning. Dette kan forebygge mer alvorlige trusler. Blokker og rapporter personer/profiler som opptrer uakseptabelt.

Reserver deg mot nummeropplysningstjenester

- Slik reservasjon og skjerming gjør deg mindre tilgjengelig, særlig for mer spontane uønskede hendelser på telefon eller i bolig. Også øvrige familiemedlemmer eller andre beboere med kjent tilknytning til deg bør skjermes. Vurder om du trenger å ha kontaktinformasjon på hjemmesiden til virksomhet, parti og lignende.

Råd til deg som mottar hets, hatefulle ytringer og trusler

Ta trusler og omfattende fiendtlighet mot deg på alvor

- Erfaringen er at truende ytringer sjelden er forbundet med reell fare. Du skal likevel ta det på alvor. Ha en plan for håndtering av slike hendelser, og følg den. Føler du deg truet, så håndter det som en trussel.

Del informasjonen med andre

- Det kan være egen (parti)organisasjon/virksomhet, leder eller sikkerhetsansvarlig. Egen organisasjon eller virksomhet har et ansvar og bør ha gode rutiner for håndtering av slike hendelser. Da må de få vite om det dersom noe skjer.

Bearbeid inntrykk og følelser, gjerne sammen med andre

- Trusler eller omfattende negativt personfokus er, eller kan over tid, utgjøre en stor personlig belastning, også for dine nærmeste. Det er derfor viktig å dele slike opplevelser. Reaksjoner, følelser og frykt kan oppstå på ulike stadier.

  Hvis du opplever at du innskrenker aktivitetene dine, begrenser deg, føler frykt eller får helseplager, bør du søke støtte. Det er viktig at politiske partier, virksomheter og tillitspersoner tilrettelegger for slike samtaler. Dine opplevelser kan også motivere andre til å åpne seg om sine opplever.

Trusler mot deg som myndighetsperson bør varsles til PST

- Gjør gjerne dette i samarbeid med egen (parti)organisasjon eller virksomhet. Det samme gjelder om du føler deg truet. Er du usikker på om en ytring er straffbar, kan det vurderes og avklares av PST.

Straffbare forhold bør anmeldes

- Politikere som ikke er myndighetspersoner kan kontakte sitt lokale politi, fortrinnsvis politikontakten i sin kommune.

3.1 | Håndtering av tilsendte trusler eller andre potensielle sikkerhetstruende henvendelser

Trusler bør sikres både av hensyn til etterforskning og for at de skal kunne vurderes og håndteres av andre, som PST eller politiet. På siste side vil du finne et skjema som kan brukes til vurdering av hvilke ytringer du bør varsle myndighetene om.

Du kan sikre digitalt fremsatte trusler ved å ta skjermbilde av ytringen der plattform og tidspunkt fremkommer. Om mulig er det fint om du kan sikre et skjermbilde av avsenderens profil og en lenke til profilen. Kontekst er viktig. Ta gjerne flere skjermbilder av et kommentarfelt og gi utfyllende informasjon, for eksempel om bakgrunnen eller rammene for hendelsen.

Av og til mottar myndighetspersoner fysiske trusselbrev. Disse bør håndteres av så få personer som mulig og med forsiktighet, samt oppbevares for eksempel i en plastpose for eventuell senere undersøkelser av politiet. For å unngå at mange håndterer brevet og ødelegger potensielle spor, kan man ta et foto av det som kan deles med andre. PST eller politiet vil vurdere sikring og beslag for eventuelle tekniske undersøkelser.

4 Informasjons-sikkerhet

Norge og norske interesser står overfor en vedvarende etterretnings-trussel fra fremmede stater.[2] Formålet er ofte å innhente informasjon om politiske prosesser som har eller kan få betydning for dem både politisk, teknologisk, militært og kommersielt. I tillegg forsøkes det å påvirke norsk politikk på alle nivåer i deres favør. Det er ofte vanskelig å forutsi hva det eksakte formålet er for etterretningsvirksomhet fra fremmede stater, og hvordan det kan få betydning i fremtiden, spesielt i et sikkerhetspolitisk perspektiv. Myndighetspersoner og politikere på alle nivåer er derfor viktige barrierer som bidrar til å beskytte samfunnskritiske verdier i samfunnet vårt.

4.1 | Etterretningstrusselen

Alle norske myndighetspersoner er interessante etterretningsmål og kan få rettet oppmerksomhet mot seg fra utenlandsk etterretning. Dette kan foregå på ulike måter. Kontaktetablering kan fremstå som legitime forespørsler, men relasjoner vil i sum og over tid kunne gjøre at man blir utnyttet mot sin vilje. Det kan foregå fordekt, slik at man ikke skal forstå hvem som står bak, eller hva som er formålet, eller ved at noen tar direkte kontakt for eksempel som ordinær diplomatisk aktivitet. Ofte brukes all tilgjengelig informasjon om deg i disse prosessene. Vær derfor bevisst på hva du deler av både jobbrelatert og privat informasjon.

Husk at det ikke nødvendigvis er myndighetspersonen selv som blir kontaktet. Det kan være noen i støtteapparatet som vil være det mest sannsynlige målet for etterretningsaktivitet. Disse vil i stor grad ha tilgang til mye av den samme informasjonen eller kan være en potensiell «bro» videre

1) PST informerer med jevne mellomrom samfunnet om hva som truer rikets sikkerhet. For oppdatert informasjon om dette henviser vi til gjeldende trusselbilde og PSTs årlige nasjonale trusselvurdering.

mot målet. Vær ekstra oppmerksom og bruk sunn fornuft om du tror at du blir kontaktet av representanter fra stater PST advarer mot i våre årlige ugraderte trusselvurderinger. Opplever du mistenkelige henvendelser eller tilnærmelser, skal egen sikkerhetsorganisasjon og PST varsles så snart som mulig.

Cyberangrep er en mye brukt metode for spionasje. Dette kan forløpe på mange forskjellige måter og fra ulike innfallsvinkler. Teknologien utvikles stadig. Etterretningsverdig informasjon er ofte lagret digitalt.

Privat og sensitiv informasjon, som bilder og meldingslogger, kan også brukes til utpressing eller påvirkning av beslutninger hvis den kommer på avveie. Det er derfor viktig at du følger oppdaterte sikkerhetsrutiner og myndighetenes råd for cybersikkerhet.

Mange av rådene som forebygger generell kriminalitet, har overføringsverdi til å forebygge etterretningsvirksomhet. Er du flink til å beskytte viktig og sensitiv informasjon, reduseres sannsynligheten for at noen stjeler den og bruker informasjonen på en uønsket måte.

Råd som kan forebygge ulovlig etterretning

Hva er skjermingsverdig informasjon?

- Gjør en vurdering av hvilken informasjon som kan være sensitiv og skjermingsverdig. Sørg for at alle med tilgang til denne har den samme forståelsen av den.

Skap en sikkerhetskultur

- Ha kontroll på og skjerm sensitiv informasjon.
- Hold deg oppdatert på myndighetenes råd og anbefalinger for bedre digital sikkerhet.
- Snakk om hva som kan skje, og om hvordan dere både kan forebygge og håndtere uønskede hendelser.
- Skjerm privatlivet ditt på internett, spesielt i sosiale medier. Dette gjør det vanskeligere å kartlegge deg og omgangskretsen din.

Vær årvåken og skeptisk

- Hvis noe føles rart eller feil, bør det følges opp. Vær oppmerksom på personer som utviser påfallende interesse for deg som person, (parti)organisasjonen/virksomheten eller arrangementer, eller som snakker med deg om andre personer.

Er du i tvil, bør du varsle egen organisasjon/virksomhet, politiet eller PST.

ID-tyveri

- Vær oppmerksom på indikasjoner på ID-tyveri. Det kan for eksempel være at noen har mottatt meldinger fra deg som du ikke har sendt, eller at det er gjennomført kredittkontroll som du ikke kjenner til. Din identitet kan misbrukes til alt fra økonomisk kriminalitet til å spre falsk informasjon i ditt navn. Varsle tidligst mulig for å begrense skade.

Verifiser dem som tar kontakt med deg

- Dagens teknologi gjør det mulig å utgi seg for å være andre på en troverdig måte, inkludert personer og virksomheter du kjenner fra før av, på både meldinger, video og telefon. Ikke åpne vedlegg eller lenker hvis noe virker rart. Er du i tvil, kan du for eksempel verifisere nye kontakter ved å ringe opp vedkommende via et sentralbord om det er mulig.

4.2 | Sikker håndtering av mobil og annet IKT-utstyr

Gjeldende råd for digital sikkerhet endrer seg raskt, og Nasjonal sikkerhetsmyndighet (NSM) er ansvarlig myndighet for nasjonale digitale sikkerhetsråd. NSMs råd er i stor grad rettet mot virksomheter, og i mange tilfeller er det derfor mest korrekt å henvise spørsmål om digital sikkerhet til egen sikkerhetsorganisasjon. Det er imidlertid noen overordnede råd i tilknytning til digital sikkerhet som sannsynligvis vil være gyldige over tid. Selv om rådene i stor grad gjelder digital sikkerhet, er det viktig å ha kontroll på sensitive dokumenter og være oppmerksom på at samtaler kan fanges opp av andre i det offentlige rom. Vær derfor svært varsom med å snakke om sensitive temaer på steder der informasjonen kan tilflyte uvedkommende.

Råd for digital informasjonssikkerhet

- Sensitive temaer eller saker bør verken diskuteres på telefon eller sendes via vanlig e-post eller SMS. Møter med sensitivt innhold bør gjennomføres uten PC, mobil og smartklokker i rommet.
- Skill tydelig mellom privat og jobb i sosiale medier, der du lagrer data, og i forbindelse med elektronisk kommunikasjon. Krypterte kommunikasjonsapplikasjoner (apper) er ofte mindre sårbare enn SMS eller e-post. Innhent råd om hvilke apper som er anbefalt eller ikke anbefalt.
- Bruk VPN; dette bidrar til å skjule datatrafikken din.
- Ikke åpne vedlegg, lenker eller QR-koder du ikke er helt sikker på. Du kan kontakte avsender for å få bekreftet at vedkommende har sendt den, eller gjøre et internettsøk for å finne ut hva det lenkes til.
- Oppgi aldri sensitiv personinformasjon, passord eller bankID til andre. Banken, myndighetene osv. vil aldri spørre om slik informasjon.
- Ha fysisk kontroll på mobiler og annet digitalt utstyr, og ikke lån det bort til andre.
- Gjør deg kjent med NSMs veiledning for hvordan man kan lage sterke passord, og bruk ulike passord til hver tjeneste.
- Bruk flerfaktor-autentisering (passord i kombinasjon med finger- eller ansiktsgjenkjenning, kodebrikke eller lignende).
- Ikke bruk USB-ladere på kollektivtransport, flyplasser og hoteller. Bruk en USB-overgang som blokkerer for dataoverføring, egen bærbar lader eller egen lader med støpsel.
- Ikke bruk ukjente USB-enheter eller minnekort.
- Oppdater alltid antivirusprogrammer, operativsystemer og apper med siste versjon av programvaren, og bruk automatiske oppdateringer der det er mulig.
- Eldre mobiler osv. får ikke alltid siste sikkerhetsoppdateringer. Det er derfor viktig å bytte ut eldre utstyr dersom leverandøren slutter med slike oppdateringer.
- Krypterer harddisker og lignende lagringsmedier.
- Gjør en kritisk vurdering før innstallering av apper, og vær restriktiv i personverninnstillingene i alle sosiale medier og apper.
- Det frarådes å tillate sporing av posisjon, eller å gi apper tilgang til kamera, mikrofon, bilder, meldinger, innstillinger, kontakter osv. utover det som er nødvendig for appens funksjonalitet. Gjør det til en vane å slette apper med tilhørende kontoer som du ikke lenger bruker.

4.3 Trådløse nettverk

Offentlige trådløse nettverk, for eksempel på hoteller og flyplasser, medfører økt risiko for cyberangrep i form av avlesing, inntrenging og kartlegging. Ved inntrenging vil uvedkommende kunne få tilgang til private data. En slik inntrenging kan også innebære at funksjoner i enheten brukes i offerets navn, som at det sendes meldinger og e-post eller publiseres innlegg i sosiale medier.

Tryggere bruk av trådløst internett

- Åpne nettverk uten passord kan overvåkes. Ikke bruk fremmede nettverk med mindre det er absolutt nødvendig, og bruk alltid VPN.
- Bruk heller mobilnett, eller et modem som er koblet til mobilnettet. Slå av Wi-Fi-tilkoblingen på enheter når det ikke er i bruk, siden enheter kan forsøke å koble seg til nettverk og oppgir informasjon når det skjer.
- Slett regelmessig lagrede nettverk du ikke lenger bruker, fra enhetene dine.
- Skjerm navn og passord på rutere du disponerer.
- Rutere har ofte mulighet for flere trådløse nettverk. Bruk et eget nettverk til «smarte dingser» i hjemmet og gjester. Unngå å bruke rutere som ikke krypterer datatrafikken.

4.4 Sikker håndtering av mobiler og tilkoblede enheter

Mobil teknologi gjør det mye enklere å være tilgjengelig i dagens teknologiske samfunn. Samtidig må man være bevisst på ulike sårbarheter som kan eksponere innholdet på mobilen eller i digitale skyer. Mobiler og brukerkontoer genererer og lagrer mye informasjon som kan havne i kommersielle databaser som selges videre, og det finnes måter å gjøre slik anonymisert informasjon tilgjengelig på. Mange apper lagrer posisjonsdata i ulike situasjoner, noe som kan hentes frem av uvedkommende. Det er derfor viktig å være kritisk til hvilke funksjoner man slår på og bruker på mobiltelefoner og nettbrett.

Sikkerhetsråd for mobiltelefoner

- Gjør deg kjent med gjeldende regler for mobilbruk via IKT- eller sikkerhetsansvarlig i din (parti)organisasjon eller virksomhet.
- På tjenestetelefon bør du kun installere programvare som er godkjent av organisasjonen/virksomheten din.
- Aktiver muligheten til å fjernslette innhold på mobilen dersom du skulle miste den.
- Gjør en omstart av mobilen jevnlig (helst en gang i uken).
- Bruk alltid passord, fingeravtrykk eller ansiktsgjenkjenning for å låse opp mobil, apper og funksjoner der det er mulig.
- Oppdater programvaren på mobilen og appene regelmessig. Ikke aksepter uventede oppdateringer du får på SMS, e-post eller tilsvarende.
- Skru av blåtann, trådløst nett og andre sendemuligheter når de ikke benyttes. Sørg for at kun godkjente kontakter kan sende noe til deg via AirDrop eller tilsvarende.
- Om mobilen inneholder sensitiv informasjon, vurder nødvendigheten av skylagring eller digitale sikkerhetskopier. Disse kan ofte bli tilgjengelige via fjerntilgang.
- Slett sensitiv historikk for anrop, e-post, SMS og kontaktlister jevnlig. Dette kan eksterne aktører få tilgang til.
- Slett innholdet på mobilen før du leverer den til service eller bytter den inn.
- Vær oppmerksom på om mobilen får avvikende adferd eller ytelse. Eksempler kan være at den bruker uforholdsmessig mye data, minne og batteri, eller at du får uventede varsler. Det kan indikere at noen har fått tilgang til den. Varsle IKT- eller sikkerhetsansvarlig i egen (parti)organisasjon eller virksomhet, og vurder å varsle myndighetene.

4.5 Varsling

Det er viktig å ha lav terskel for å varsle om mistenkelig eller uvanlig aktivitet som kan være relatert til etterretningsaktivitet og informasjonssikkerhet. Graden av behov for hjelp (disponibel tid, det akutte i situasjonen osv.) avgjør hvem du kontakter.

Pågående datainnbrudd

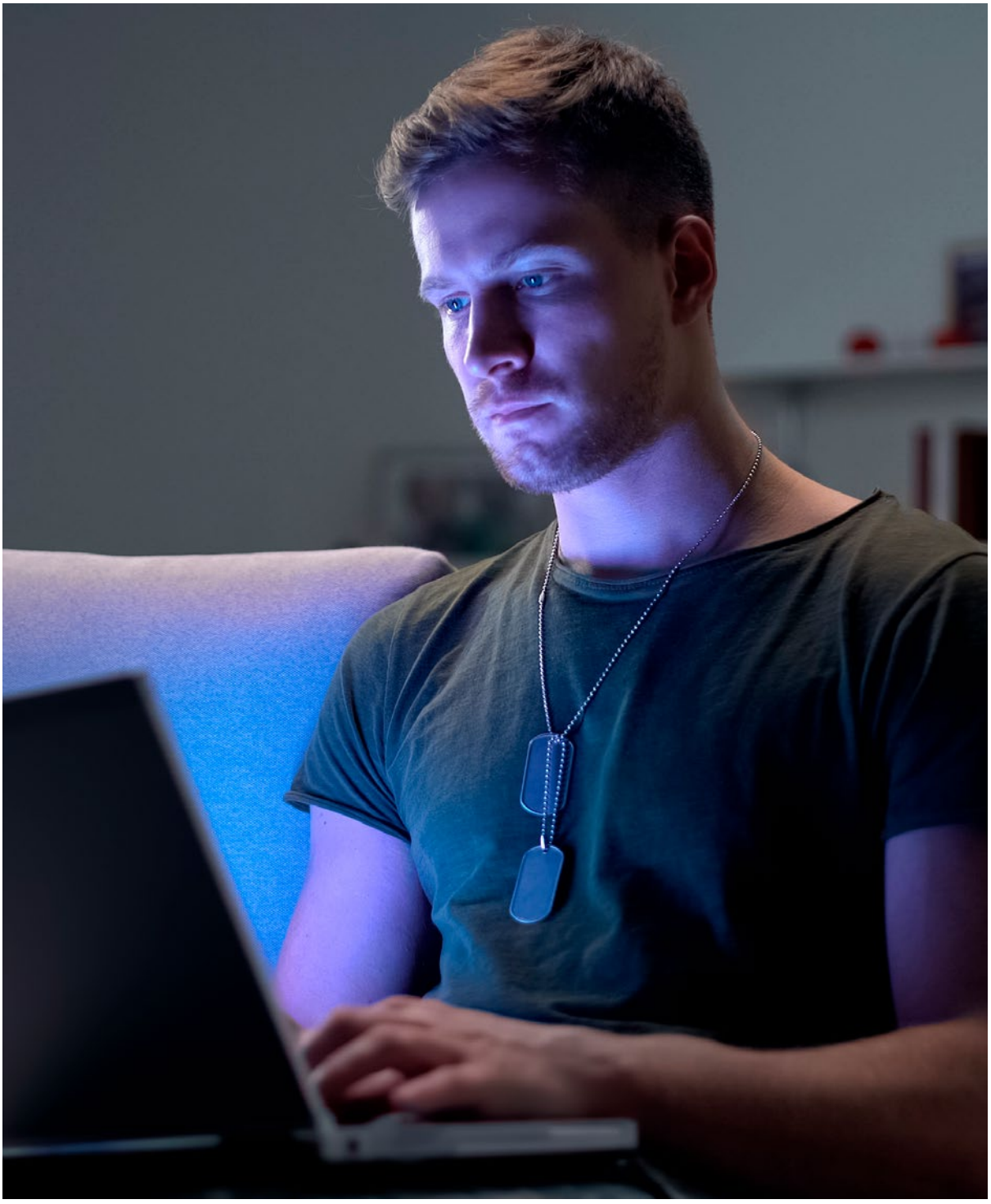
- Varsle (parti)organisasjonens eller virksomhetens IKT- eller sikkerhetsleder som har etablerte kanaler til NSM.
- Varsle politiet.

Ved mistanke om at noe er galt

- Har du indikasjon på at noe er galt med tanke på digital sikkerhet, bør du varsle dem som administrerer utstyret (ofte virksomheten eller organisasjonen), samt IKT- eller sikkerhetsleder.
- Fremstår det som et lovbrudd, bør politiet varsles og anmeldelse vurderes.

Mistenkelig tilnærming

- Hvis du mistenker at utenlandsk etterretning kontakter deg, eller opplever at noen viser påfallende interesse for deg og ditt virke, bør du drøfte dette med en ansvarlig i egen (parti)organisasjon eller virksomhet, og deretter varsle PST.
- Vurder eventuelt å varsle organisasjonen/virksomheten og dine nærmeste der det er naturlig.
- PST kan gi spesifikke råd ut fra en vurdering av situasjonen hvis du er usikker.




眼鏡
OPTICAL
SK-II

5 Sikkerhet på reise

Ved reiser til utlandet kan du komme i situasjoner der din eller medreisendes sikkerhet blir truet. Det finnes mange måter du kan oppnå bedre personlig sikkerhet på, og noe av det viktigste er å gjøre gode forberedelser før reisen starter.

5.1 | Personlig sikkerhet

Personsikkerhet og vurdering av sikkerhetstiltak bør inngå i planleggingen og gjennomføringen av alle reiser, spesielt til områder som kan ha et mer alvorlig trusselbilde enn Norge. På utenlandsreiser kan trusler eller farer knyttet til høy kriminalitet, terrorisme og kidnapping, naturkatastrofer, trafikksikkerhet, infrastruktur, helseutfordringer og/eller etterretningsvirksomhet oppstå. Trusselbildet for regioner, land og områder er forskjellig. En normal sikkerhetssituasjon kan endre seg raskt til å bli utrygg og/eller uforutsigbar. På Utenriksdepartementets (UD) nettside med reiseinformasjon kan du innhente opplysninger om sikkerhetssituasjonen i landet du skal reise til. UD tilbyr også reiseregistering, noe som gjør at norske myndigheter kan ha oversikt over reisende som oppholder seg i et gitt land, samt bidrar til at man raskt vil kunne varsle ved ekstraordinære hendelser.

Kapittelet inneholder ingen uttømmende liste over hva du skal og ikke skal gjøre for å unngå eller håndtere en sikkerhetstruende eller annen uønsket hendelse. Rådene må vurderes for hver enkelte reise. Tilpasninger eller andre tiltak kan være hensiktsmessig.

Før avreise

- Det anbefales at det utpekes en ansvarlig for reisen. Vedkommende vil for eksempel kunne
  - lage en oversikt over nødvendige vaksiner
  - etablere kontakt med den norske ambassaden
  - sette opp en oversikt over praktiske spørsmål i forbindelse med reisen
  - lage en liste med viktige telefonnummer i besøkslandet
  - utpeke felles samlingssted ved uforutsette hendelser
  - kartlegge ulike transportmidler under oppholdet
  - opprette en kryptert chat for reisefølget
- Innhent beredskapsplaner hvis det er utarbeidet for reisen, og gjør deg kjent med dem.
- Sett deg inn i situasjonen i området du skal besøke. Tenk gjennom hva du vil gjøre hvis noe uforutsett skulle inntreffe.
- Ta med deg gyldige reisedokumenter og nødvendig utstyr, for eksempel enkelt førstehjelpsutstyr, reiseapotek, bærbar lader, strømadapter, lommelykt og kontanter.
- Innhent viktige telefonnummer (norsk ambassade, lokalt politi, norske myndigheter osv.) og lagre disse på mobilen.
- Ta i tillegg med en fysisk kopi av pass, kredittkort, reisedokumenter og nødvendige kontaktinformasjon (i tilfelle du mister mobilen din).
- Sørg for å ha en reiseforsikring som gjelder for besøkslandet.

Sikkerhetsråd under reise og transport

- Opphold deg kortest mulig tid i avgangshallen før du går gjennom sikkerhetskontrollen til mer sikkert område.
- Ha kontroll på din egen bagasje, og sjekk om noen har åpnet eller forsøkt å åpne den.
- Tyverier skjer spesielt under transport, på flyplasser og på spisesteder.
- Hvis mulig, hold deg sammen med reisefølget ditt.
- Vær presis ved transport til og fra besøkssteder.
- Unngå å sette deg i en situasjon der vurderingsevnen blir vesentlig redusert (for eksempel ved bruk av rusmidler).
- Undersøk hvilke transportmidler som er anbefalt benyttet, for eksempel anbefalte drosjeselskap eller Uber, og følg anbefalingen.

På hotellet

- Ha oversikt over hvor alle i reisefølget bor.
- Etter ankomst til hotellet bør du gjøre deg kjent med hotellets sikkerhetsrutiner, nødutganger og nærmeste brannslukkingsutstyr.
- Om mulig, samle reisefølget slik at alle bor i samme etasje og helst ved siden av hverandre. Be om at rommene ikke er på bakkeplan, men fortrinnsvis i 3. til 5. etasje, og helst ikke direkte over resepsjonen.
- Vurder å bytte rom, etasje eller hotell dersom du føler deg utrygg.
- Avtal et sikkert sted der reisefølget skal møte ved en uforutsett hendelse. Det kan være det mest egnende rommet dere har. Unngå resepsjonen.
- Lås døren og bruk alltid sikkerhetslenken når du er på hotellrommet.
- Vær oppmerksom på at hotellrom, møterom, fasttelefon og mobil kan bli avlyttet. Skjult videoovervåking av rom kan også forekomme.
- Ta med en røykvarsler beregnet for reiser.

I det offentlige rom

- Vis respekt for kultur, religion og tradisjon i landet du besøker.
- Sørg for å vite hvor du er til enhver tid, og noter deg navn og adresse på hotellet ditt.
- Om du må forlate reisefølget ditt, meld fra hvor du skal. Informer om hvordan de kan komme i kontakt med deg, og om når du planlegger å være tilbake.
- Gjør deg kjent med og vær oppmerksom på omgivelsene dine. Dersom du føler deg utrygg, oppsøk hjelp eller gå inn på et trygt sted (for eksempel hotell, politistasjon eller lignende) eller søk hjelp på annen måte.
- Ha mobiltelefonen med deg.
- Unngå å oppsøke områder og situasjoner som kan utvikle seg til å bli truende (kriminalitet, demonstrasjoner og opptøyer).
- Unngå oppmerksomhet fra kriminelle. Vis aldri frem penger eller verdisaker. Pass på tingene dine.
- Situasjoner som kan brukes som et pressmiddel mot deg, kan bli fremprovosert. Om man er flere sammen, reduseres risikoen for å bli utsatt for denne typen hendelser.
- Dersom du opplever ubehagelig tilnærming av politi, sikkerhetspersonell eller tilsvarende, må du opptre korrekt. Forsøk likevel å unngå å bli dratt inn i en vanskelig situasjon.
- Tenk over hva du sier, og hvor du sier det; du kan være under observasjon. Ikke la andre se hva du jobber med på PC og nettbrett.
- Lokalt ansatte ved norske virksomheter i utlandet kan bli utnyttet eller brukt som informanter. Vær bevisst på hva du deler, og hva du snakker om i deres nærvær.
- Uønskede hendelser bør rapporteres til norske myndigheter.

Truende situasjoner

Hvis du blir utsatt for en truende hendelse, for eksempel provokasjon, forulempning, fysisk angrep, ran eller gisseltaking, vil reaksjonene dine være viktige for både deg selv og de du er sammen med. Reaksjonsformen må stå i forhold til trusselens alvorlighet og den konkrete situasjonen.

- Forsøk å komme deg vekk fra en truende situasjon og oppsøk et trygt sted.
- Behold roen, vær høflig og opptre korrekt. Dette kan påvirke gjerningspersonen positivt.
- Hvis du ikke kan komme deg unna situasjonen, påkall andres oppmerksomhet.
- Adlyd de ordrene som blir gitt. Det er bedre å gi fra seg lommebok, veske eller andre verdigjenstander enn å holde disse tilbake. Gjør motstand hvis du må.

Spesielt om gisselsituasjoner

- Gjør som du får beskjed om.
- Gisseltakerne er også stresset og kan anse deg som en trussel.
- Forsøk å varsle norske myndigheter eller andre om at du er tilbakeholdt, så raskt som mulig.
- Forvent røff behandling, mye støy og en uoversiktlige situasjon.
- Forsøk å bevare roen og snakk rolig og tydelig. Svar på eventuelle spørsmål.
- Forsøk å bygge gode relasjoner til gisseltakerne.
- Be om medisiner, mat, drikke eller andre ting som du måtte trenge.
- Forvent å bli fratatt gjenstander.
- Forvent at du blir overvåket, også elektronisk.
- Selv om det vil bli iverksatt et stort apparat for å hjelpe deg, må du selv aktivt forsøke å forbedre din egen situasjonen.

5.2 | Reiser med særlig forhøyet risiko for liv og helse

Noen reiser krever ekstra forberedelse og beredskap for uønskede trusselhendelser. Det kan være flere kjente grunner til dette, alt fra høy terrortrussel til helsefarer og begrensende muligheter for forsvarlig medisinsk behandling. For myndighetspersoner som i tjeneste reiser til land med et særlig skjerpet trusselbilde, på såkalt høyrisikoreise, vil PST gjøre en konkret risikovurdering med anbefalte sikkerhetstiltak og gi sikkerhetsråd.

Sikkerhetsrådene som er nevnt tidligere i håndboken, gjelder også for reiser til risikoutsatte områder. I tillegg bør følgende råd følges:

Før reisen

- Innhent informasjon om sikkerhetssituasjonen i området du skal besøke.
- Informer relevante myndigheter, som PST og Utenriksdepartementet.
- Gjennomfør et sikkerhetsmøte, og vurder og gjennomgå konkrete sikkerhetstiltak og -utstyr.
- Ta med personlig førstehjelpsutstyr, medisiner og reiseapotek.
- Vurder å ta med satellittelefon.

Under reise og transport

På reiser er det som oftest transportetappene som er mest risikoutsatt.

- Vær oppmerksom på omgivelsene dine. Begrens bruk av hodetelefoner/øreplugger. Det kan forhindre deg fra å oppfatte viktige meldinger eller truende situasjoner.
- Vent innendørs til alle er til stede og transporten er klar.
- Hold dører og vinduer lukket under transport.
- Hold deg oppdatert på sikkerhetssituasjonen. Den kan endre seg.
- Følg med på lokale og internasjonale nyheter.
- Ved ekstraordinære hendelser bør du følge instruksene fra lokale myndigheter.
- Bruk utlevert sikkerhetsutstyr når du får beskjed om det (vernevest, hjelm osv.).

På hotellet

Etter ankomst til hotellet:

- Om mulig bør du gjøre deg kjent med og prøve evakueringsruten for å se at den fungerer. Vær obs på dører med alarm.
- Merk deg plassering av tilfluktsrom eller sikre rom.
- Ha en reiseveske (grabbag) med nødvendig utstyr lett tilgjengelig i tilfelle evakuering. Reisevesken bør inneholde lommelykt, utlevert sikkerhetsutstyr, vann, lettere proviant, pass, kredittkort, ekstra klær og eventuelle sensitive dokumenter. Vurder å ha med en flaske med vannrensefilter, eller tabletter som renser vann.
- Sjekk telefonforbindelsen hjem, til andre i følget og til hotellets resepsjon.
- Ikke gi fra deg eller på annen måte eksponer romnummeret ditt for uvedkommende. Husk at romnummeret kan stå på nøkkelen.
- Begrens innsynet til hotellrommet.

I det offentlige rom

- Unngå opphold i det offentlige rom så langt som mulig. Respekter pålagte begrensninger i din bevegelsesfrihet.
- Gå flere sammen dersom dere må oppholde dere utendørs i det offentlige rom.
- Opptre diskret og hold en lav profil; ikke oppgi virksomhet, (parti)organisasjon eller stilling utover det mest nødvendige. Forsøk å kle deg anonymt slik at du glir inn i folkemengden. Prøv å ikke se «militær» eller velstående ut; dette kan øke oppmerksomheten rundt deg.
- Plasser deg slik at du har oversikt over restaurantlokalet, bussen, folkemengden osv. der du til enhver tid befinner deg.
- Følg med på omgivelsene og vurder hvordan du kan trekke deg unna dersom en truende situasjon oppstår.

Etter reisen

- Hvis det har oppstått sikkerhetstruende eller problematiske situasjoner under reisen, informer om dette til (parti)organisasjonen eller virksomheten din umiddelbart etter hjemkomst.

5.3 | Terrorangrep eller livstruende situasjoner

I enkelte land, regioner og byer er det større risiko for terrorangrep og andre alvorlige voldshandlinger. I slike tilfeller er det viktig å bevare roen, men samtidig ta trusselen på alvor. De første sekundene kan være avgjørende for om man kommer uskadet fra en livstruende situasjon. Dersom du ledsages av sikkerhetspersonell, må du følge deres råd og ordrer

Grunnleggende råd ved terrorangrep:

1. Flykt

- Vurder situasjonen og mulighetene, ta initiativ og handle.
- Kom deg bort fra området. Ikke ta med deg noe unødvendig, og hold hendene synlig. Advar andre.
- Dersom terrorangrepet startet med en eksplosjon, må du være oppmerksom på andre farer, som branner, gasslekkasjer og ødelagte bygninger.
- Vær forberedt på at ytterligere angrep kan inntreffe, for eksempel fra bevæpnede terrorister.

2. Søk dekning

- Dersom det ikke er mulig å rømme, eller du er i nærheten av gjerningspersonene, finn et sikkert gjemmested som kan låses eller barrikaderes.
- Lås, slukk lyset og vær stille. Hold deg unna vinduer og dører til faren er over.
- Skru av all lyd og vibrering på mobilen, og skru ned lysstyrken på skjermen for ikke å avsløre hvor du er.
- Ikke ring unødvendig til personer som kan befinne seg i området, det kan utsette dem for fare.
- Ikke forlat gjemmestedet før politiet har gitt klarsignal.
- Skjul og dekning er ikke alltid det samme: Husk at «ute av syne» ikke betyr at du ikke kan rammes av skudd.
- Dersom du ikke har annet valg og det står om livet, angrip gjerningspersonen med alle tenkelige hjelpemidler.

Flykt – Søk dekning – Varsle

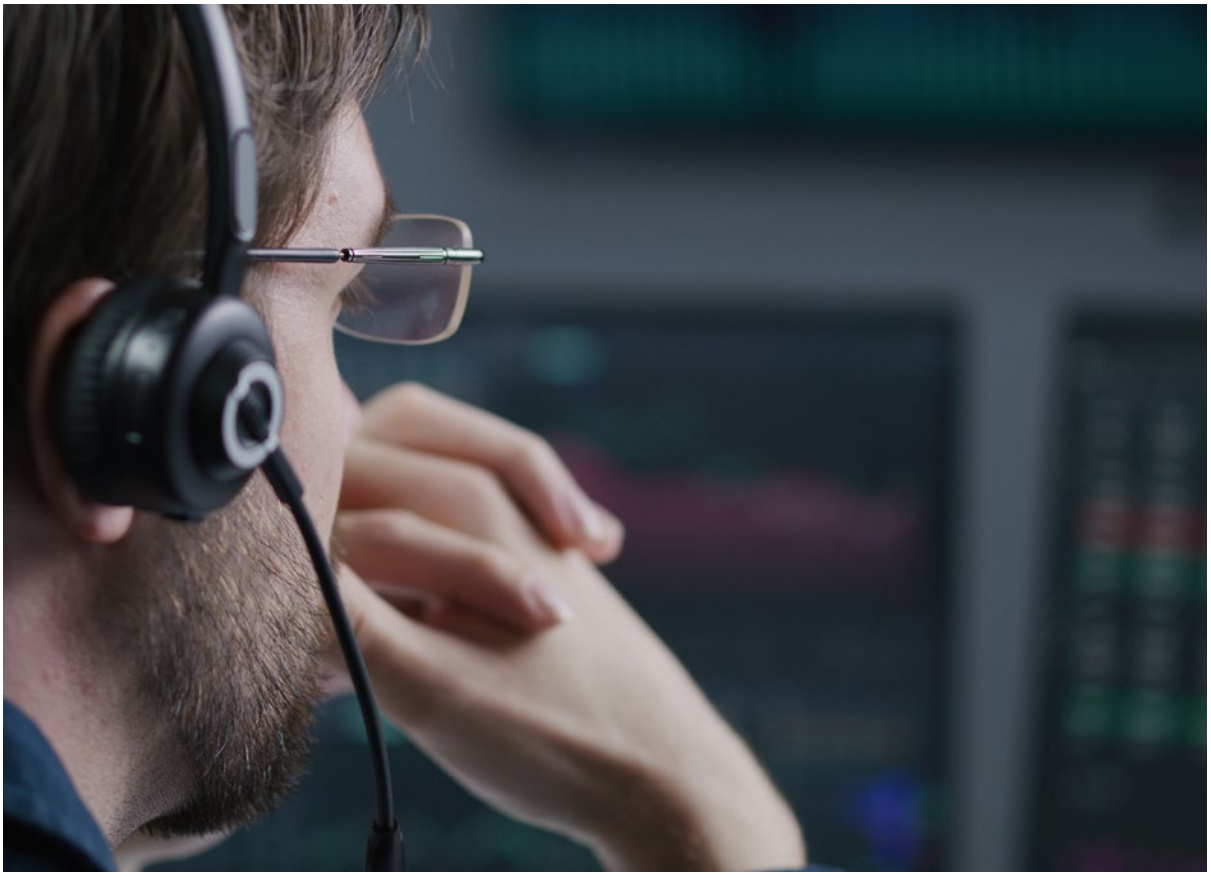
3. Varsle

- Varsle politiet så raskt som mulig, alternativt send melding til noen som kan ringe for deg. Du kan ha viktig informasjon som gir politiet forutsetninger for å stanse angrepet.
- I en alvorlig situasjon kan telenettet overbelastes. Det kan være vanskelig å ringe politiet. I slike tilfeller kan meldinger ofte fortsatt brukes. Noen apper gir stedslokasjon til nødetatene.
- Kan du ikke snakke, kan du ha en åpen linje på telefonen slik at politiet kan lytte til hva som skjer
- Følg politiets anvisninger. Når politiet kommer til stedet, er det viktig at du opptrer rolig og ikke på en måte som kan oppfattes som at du kan være en gjerningsperson. Ikke ha noe i hendene og hold dem synlig for politiet. Forhold deg rolig, og vær forberedt på at du kan bli pekt på med skytevåpen.

5.4 | Informasjonssikkerhet på reise med forhøyet etterretningstrussel

Fremmede sikkerhets- og etterretningstjenester kan ha større handlingsrom til å innhente informasjon om deg i utlandet. I land som utgjør en særlig etterretningstrussel mot Norge, land der disse har stor tilstedeværelse, og totalitære stater for øvrig vil sikkerhets- og etterretningstjenester ha lav terskel og betydelig kapasitet for målrettet etterretningsvirksomhet. Virksomheten kan rettes mot både deg og personer du er i kontakt med. Aktiviteten kan for eksempel være i form av hemmelig ransaking, avlytting, overvåking av trådløst nett, innhenting av teletrafikk og fysisk kontroll av deg og din bagasje. Som myndighetsperson må du ta for gitt at besøket er kjent for sikkerhets- og etterretningstjenestene i transittland og på destinasjonen.

Ved reiser til utsatte land bør det gjøres en vurdering av i hvilken grad og på hvilken måte skjermingsverdig informasjon skal medbringes og eventuelt oppbevares. Dette er en forutsetning for eventuelle sikkerhetstiltak. Gjør deg kjent med egen organisasjons/virksomhets retningslinjer for bruk av IKT-utstyr på reiser til utlandet og følg disse.



Råd for informasjonssikkerhet før reisen

- Ved høy risiko anbefales det å ta med utstyr som kun benyttes på reisen.
- Ved lavere risiko kan det utstyret man benytter til vanlig, tilpasses.
- Ta med minst mulig sensitiv og skjermingsverdig informasjon. Oppdater og forbered utstyret du skal ta med.
- På nsm.no finnes utfyllende råd for digital sikkerhet på reiser.

Råd for informasjonssikkerhet under reisen

- Overføringsfunksjoner som trådløst nett og blåtann bør slås av når de ikke er i bruk. Bruk aldri offentlige trådløse nett i utlandet. Bruk mobildata eller mobilt bredbånd.
- Ikke last ned programvare eller oppdateringer under reisen med mindre det er viktige sikkerhetsoppdateringer.
- Ikke legg igjen digitalt utstyr eller sensitiv informasjon på hotellrommet. Forutsett at alle ansatte på hotellet har tilgang til både rommet og safen.
- Benytt forseglingspose hvis du må legge fra deg ditt digitale utstyr.

Råd for informasjonssikkerhet etter hjemkomst

- Hvis du har hatt spesialutstyr for reisen, fortsett å holde utstyr og data adskilt fra eget og hjemlig utstyr.
- Fortsett å være kritisk til uventede og ukjente sikkerhetsvarsler, e-poster, vedlegg og bilder.
- Har du vært utsatt for tilnærming eller annen kontakt fra etterretnings- og sikkerhetstjenester, bør dette rapporteres i egen virksomhet/organisasjon og til PST.
- Vær oppmerksom på at du etter reiser kan motta henvendelser fra etterretningspersonell på e-post eller sosiale medier med ønske om videre kontakt. Informer PST dersom dette skjer.

Kilder

Håndboken er skrevet og publisert av Politiets sikkerhetstjeneste. Rådene støtter seg også på andre relevante sikkerhetsmyndigheter. Lenker til konkrete råd utgitt av andre sikkerhetsmyndigheter er lagt inn i teksten der disse er relevante og vist til.

NSM har mer inngående informasjon og rådgivning, særlig hva gjelder digital sikkerhet, kommunikasjonssikkerhet og informasjonssikkerhet. Dette er tilgjengelig på nsm.no.

På Utenriksdepartementets (UD) hjemmesider finner du reiseinformasjon om innreise, naturforhold og andre relevante opplysninger for nær 200 land. Reiseregistrering.no er et tilbud om å registrere kontaktopplysninger hos UD. Dersom det skjer en alvorlig hendelse, har UD mulighet til å sende deg informasjon på SMS eller e-post. Utenriksdepartementet gir også reiseråd når de mener at norske borgere ikke bør dra til et land eller et område.

På Kommunal- og distriksdepartementets hjemmesider finner du informasjonom norske lokalpolitikeres erfaringer med trusler, hatytringer og plagsomme henvendelser. Her finner du også *Veileder om forebygging og håndtering av hatefulle ytringer, hets og trusler mot politikere og kandidater,* og *Gode sikkerhetsråd til deg som stiller til valg,* som er utarbeidet av Etterretningstjenesten, NSM og PST i samarbeid med departementet.

Varsling

Varsling om trusler

- Hvis det er fare for liv og helse, ring politiets nødnummer **112**.
- Ved andre straffbare forhold eller bekymringer, ring **02800**, som går til politiet der du er.
- Trusler mot myndighetspersoner (som ikke er akutte) varsles i etablerte kanaler eller til PSTs døgnåpne responssenter: **23 30 50 00 / post@pst.politiet.no**
- Det er også mulig å sende en e-post til både PST og politiet selv om det ikke foreligger en konkret trussel. Potensielt sikkerhetstruende forhold kan være sammensatte og utvikle seg over tid. Kunnskap om slike forhold er relevant for PST og politiet, som grunnlag for både konkrete sikkerhetsvurderinger og tiltak, og opprettelse av straffesaker.

Mottaksvurdering for bekymringsfulle hendelser

Skjemaet gir veiledning for å identifisere hendelser, henvendelser eller ytringer fra personer eller aktører, som bør noteres og rapporteres internt og eventuelt varsles til politiet eller PST.

Informasjon om hendelser bør ringes inn eller helst sendes skriftlig til PST eller politiet. Dersom hendelsen knyttes til særlig sensitive eller skjermingsverdige forhold, kan det avtales et fysisk møte med PST.

Ved fare for akutte trusler skal politiet varsles ved å utløse alarm eller ved å ringe 112.

	Det foreligger informasjon om eller en person/aktør uttrykker eller fremsetter følgende:	Ja	Nei
1	Trusler eller truende henvendelser.		
2	Voldelige tanker, planer eller fantasier, eller referanser til andre voldshendelser eller våpen.		
3	Suicidale tanker.		
4	Uttalelser om at dette er «siste utvei» eller at dette er «siste sjanse».		
5	Vrangforestillinger om å være truet på livet eller om tap av kontroll over eget liv.		
6	Person(er) oppsøker deg på en mistenkelig måte, på private arenaer, arrangementer, arbeidssted eller det fremkommer informasjon/trusler om dette.		
7	Skadeverk på eiendeler/eiendom eller innbrudd.		
8	Unormalt sinne, opprørthet eller seksuelt krenkende atferd.		
9	Noen har privat informasjon som ikke er eller burde vært kjent, om deg, kollegaer eller andre relevante personer.		
10	Innbilt spesiell personlig relasjon til deg, kollegaer eller andre relevante personer.		
11	Vedkommende tror han/hun er Gud, har et gudommelig oppdrag e.l.		
12	Svært stort antall henvendelser fra samme person.		
13	Flere henvendelser fra samme person som blir mer aggressive eller merkelige.		
14	Vedkommende har skapt uakseptable problemer tidligere.		

(1–6 = varsle PST eller politiet)

(7–14 = varsle internt. Vurder å varsle PST eller politiet særlig ved flere forhold.)


PST
POLITIETS
SIKKERHETSTJENESTE