

Personlig sikkerhet



**En veileder for myndighetspersoner
og andre risikoutsatte**



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



Innhold

Side

1.	Sikkerhet er et felles ansvar	5
2.	Trygghet i hverdagen	9
3.	Sjikane, hets og trusler	23
4.	Informasjons-sikkerhet	29
5.	Sikkerhet på reise	37

■	Varsling	50
■	Kilder	50
■	Vurdering av bekymringsfulle hendelser	51



1

Sikkerhet er et felles ansvar

PST har et særskilt ansvar for å forebygge og etterforske trusler mot landets myndighetspersoner. Samtidig hviler det et ansvar på den enkelte, deres virksomhet, parti eller organisasjon til å bidra til en god sikkerhet. Det er grunnleggende for vårt demokrati at myndighetspersoner kan utføre sine oppgaver på en trygg og sikker måte. Denne håndboken har som formål å 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 er det samlet informasjon og veiledninger som har til formål å øke sikkerhetsbevisstheten og tryggheten for deg som myndighetsperson. Håndboken er delt inn etter utvalgte temaer og arenaer der du kan være trussel og risiko utsatt. Hvert tema har tilhørende råd om forebyggende sikkerhetstiltak og/eller handlingsmønstre

som kan redusere konsekvensene hvis uønskede hendelser likevel skulle oppstå.

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

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

1.1 | Risiko som en del av hverdagen

Det er i utgangspunktet trygt å være politiker i Norge. Det kan likevel være situasjoner hvor din sikkerhet kan bli utfordret. Hva du bør gjøre, vil avhenge av situasjonen du befinner deg i. Sikkerhetsrådene kan derfor regnes som forholdsregler som vi tar på samme måte som det å være årvåken i trafikken og å bruke bilbelte. I et demokrati er det viktig for de

folkevalgte å være tilgjengelige for velgerne. Sikkerhetsrådene i denne veilederen tar derfor sikte på å ikke være til hinder for din politiske virksomhet, men skal styrke dine forutsetninger for å vurdere risiko og eventuelt redusere den til et akseptabelt nivå.

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 på et arrangement der du kan være mer utsatt enn normalt.

Uønskede hendelser kan oppstå når

- Du/dere er involvert i kontroversielle saker med stor medieoppmerksomhet hvor enkelte har sterke personlige interesser eller er sterkt følelsesmessig berørt.
- 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 din. Vær bevisst på når, hvor og hvordan du kan være sårbar for ulike trusselaktører.
- Vær mentalt forberedt på at sikkerhetstruende hendelser kan oppstå.
- Søk råd hos personer i egen (parti)organisasjon/virksomhet, sikkerhetsansvarlige, PST eller politiet om du er usikker.
- Håndter sensitiv informasjon slik at den ikke blir tilgjengelig for andre.
- Varsle eget (parti)organisasjon/virksomhet, sikkerhetsansvarlige, PST eller politiet dersom du utsettes for trusler eller sikkerhetstruende hendelser. Det er viktig at du ikke står i denne typen hendelser alene.

1.2 | Risikoforståelse

Det finnes flere ulike måter å beskrive risiko på. I denne håndboken ser vi på risiko som en kombinasjon av faktorene verdi, trussel og sårbarhet. For deg som myndighetsperson vil rutinemessige og strukturerte risikovurderinger, med eventuelle nødvendige risikoredukerende tiltak, ofte ha en betydelig positiv innvirkning på risikoen for deg. Både ved

å redusere sannsynligheten for at en sikkerhetstruende hendelse finner sted, og at skadefølgen blir minst mulig dersom en slik hendelse likevel skulle inntreffe. Det krever at du og ditt støtteapparat har grunnleggende kjennskap til det rådende trusselbildet, en god forståelse av dine egne verdier og hvordan både du og dine interesser er sårbare.





2

Trygghet i hverdagen

Truende hendelser kan gjøre alvorlig skade både for deg som utsettes for dem, men også for ditt virke, familien, andre nærstående og på samfunnet for øvrig. Sannsynligheten for at en truende hendelse skal oppstå og at det dermed oppstår et behov for sikkerhetstiltak vil variere fra person til person. Behovet for sikkerhetstiltak vil også avhenge av hvilken posisjon du har. PST anbefaler at alle myndighetspersoner er sikkerhetsbevisste både i jobb og på fritiden.

Eksempler på scenarioer som kan inntreffe i hverdagen

- Noen kommer helt opp i ansiktet på deg, kjefter og er så nærgående at du blir dyttet om du ikke trekker deg 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 og banker på døren din og insisterer på at du skal åpne.
- Noen utfører hærverk på boligen din, bilen eller på andre eiendeler.

2.1 | Familie og sikkerhet

Trusler mot deg som myndighetsperson vil også kunne ramme eller påvirke familien og dine nærmeste. God sikkerhet bygges i fellesskap.

Snakk om sikkerhet

- Du bør informere de rundt deg dersom din posisjon gjør deg risikoutsatt eller ved endringer i risikobildet.
- Vær likevel oppmerksom på at trusselinformasjon eller stort sikkerhetsfokus kan medføre unødvendig utrygghet for noen. Du kan derfor tenke på sikkerhetstiltakene som nødvendige, men viktige forholdsregler. For eksempel på samme måte som du forbereder deg på at det kan bli dårlig vær når du ferdes i fjellet.
- Personalet i barnehagen, på skolen og på fritidsaktiviteter til barna dine bør informeres og oppdateres om nye rutiner. For eksempel bør de som skal hente barn ikke være ukjente for personalet. Vi er ofte mer sårbare når vi er alene. Legg derfor til rette for at barn kan gå sammen med venner eller en voksen til og fra skolen og fritidsaktiviteter.
- Legg til rette for at dine nærmeste forteller deg om uvanlige hendelser og at de deler eventuelle bekymringer som de måtte ha med deg.

2.2 | Vær sikkerhetsbevisst ved opptredener på offentlig sted

Støtteapparatet rundt deg som myndighetsperson kan aktivt bidra til å øke sikkerheten. Ved planlagte møter med publikum kan god dialog i forkant med arrangøren og andre

involverte aktører være viktig både for å fremme felles sikkerhetsbevissthet, for å innhente relevant informasjon og for tilrettelegging av sikkerhetstiltak.

Vurderinger ved offentlig tilgjengelige arrangementer

Det er flere forhold som kan innvirke på risikoen ved et offentlig arrangement. Punktene under kan brukes for å vurdere risikoen og behovet for forebyggende tiltak.

- Hvem er arrangør og hvem er ansvarlig for sikkerheten på stedet?
- Er det en økt fare for at det oppstår sikkerhetstruende hendelser?
- Foreligger det en handlingsplan dersom noe skulle skje?
- Vil det være politi og/eller sikkerhetsvakter til stede?
- Er det andre deltakere til stede som kan tiltrekke seg uønskede personer?
- Er stedet eller området belastet på noen måte?
- Vil det være forhåndspåmelding og/eller adgangskontroll?
- Er det andre myndighetspersoner til stede?
- Er området rundt scenen og venteområdet avgrenset eller avspærret?
- Er det behov for å varsle PST eller politiet i forkant av arrangementet? Det kan i noen tilfeller være at myndighetene har relevant informasjon eller vil vurdere egne tiltak.

Sikkerhetsråd for opptreden i det offentlige rom

Ha oversikt over publikum og ryggen fri

- Forsøk å skape en terskel eller avstand mellom deg selv og publikum, eksempelvis ved bruk av en talerstol, et bord eller sperrebånd og lignende. Slike terskler kan virke forebyggende og de kan gi deg et forhåndsvarsel dersom en person likevel velger å krysse dem.
- Være kritisk til å motta og åpne pakker eller andre gaver du ikke vet hva er. Du kan eventuelt be giveren om å selv pakke den opp, eller overlevere den til det ordinære postmottaket.
- Følg jevnlig med på de andre i gruppen din for å kunne oppdage om noen trenger støtte eller hjelp.
- 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.

Vær forberedt på forstyrrelser

- Ha alltid med mobiltelefon og alarm (hvis du har det). Tenk gjennom tiltak og rollefordelinger med de andre i gruppen din på forhånd.
- Hvis noen opptrer forstyrrende eller truende, er det best å unngå å provosere vedkommende ytterligere. Trekk deg heller unna til situasjonen er håndtert av andre.
- Gjør deg kjent med planlagt vei inn og ut av et møtested, samt alternative rømningsveier. Slik kan du raskt forlate en farlig eller uønsket situasjon og komme deg i sikkerhet.
- Gitt en truende eller uønsket hendelse skulle oppstå så er det en stor fordel om du kan forlate stedet uten å måtte gå gjennom publikumsområdet.

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

- Tenk hvor dine grenser går og praktiser grensesetting i både det fysiske og det digitale rom.
- Øv deg på å avslutte uønskede samtaler på en høflig, men bestemt måte og helst på et tidlig tidspunkt. Dette kan forebygge at situasjoner utvikler seg til hets, hatefulle ytringer og trusler. Gi beskjed om hvorfor samtalen avsluttes, for eksempel at vedkommende oppleves som truende. Om mulig så vær også tydelig på at fremtidige henvendelser vil bli avvist og rapportert.

Opptre sammen

- Potensielle trusselaktører vil ofte ha en høyere terskel for å konfrontere deg dersom dere er flere som er sammen. Det gir dere også muligheten for å støtte og avlaste den av dere som blir konfrontert eller utsatt for annen uønsket adferd. Det å være flere sammen gjør det også enklere å varsle om situasjonen som har oppstått.

Bruk av bil gjør deg mindre sårbar

- Utsatte myndighetspersoner bør på generelt grunnlag begrense bruken av kollektivtransport, spesielt i bysentrum. Ombord på en buss, trikk eller et tog er du forholdsvis fastlåst og dermed mer sårbar. Muligheten for å kunne trekke deg unna en situasjon er betydelig redusert.
- Et kjøretøy kan også fungere som et trygt sted å trekke deg tilbake til dersom en uønsket hendelse skulle oppstå.

Bruk av drosje

- Bruk av drosje kan være et godt forebyggende sikkerhetstiltak.
- Drosje eller tilsvarende transporttjenester bør helst bestilles på forhånd.
- Vent med å gå ut til drosjen til den har ankommet.

Skjerming av informasjon

- Ankomsttid, sted, hvordan du ankommer og hvor du oppholder deg før og etter arrangementet er opplysninger som en potensiell trusselaktør kan utnytte. Denne typen informasjon bør vanligvis skjermes og ikke forhåndsannonseres.
- I særlige tilfeller bør du vurdere å vente med å offentliggjøre deltagelsen din til etter at et møte eller arrangement har blitt gjennomført.

2.3 | Forebyggende sikkerhetstiltak for egen bolig

Ditt eget hjem er det stedet du oppholder deg mest. Samtidig kan det være mange som vet eller som kan finne ut hvor du bor. Vær derfor forberedt på at din egen bolig kan være et sted der potensielle trusselaktører kan oppsøke deg.

Det er flere sikkerhetstiltak som kan iverksettes for å sikre boligen din og gjøre deg mindre sårbar. De fleste tiltakene må dere

følge opp selv. Gjør deg derfor kjent med boligen din ut fra et sikkerhetsperspektiv. Hvilke sårbarheter har den og hvilke tiltak bør utføres? Som myndighetsperson kan du få råd om sikring av boligen din fra vakt-selskap, politiet eller av PST. For mange holder det med forholdsvis enkle tiltak. For andre er det behov for mer inngripende tiltak.

Skallsikring, dører og vinduer

- Har du en brevluke i ytterdøren så bør denne stenges eller at du installerer en brannsikker kasse på innsiden av brevluken.
- Vær bevisst på om vinduer og dører er åpne. Lukk og lås dem når ingen er hjemme. Husk at et vindu som er «låst i åpen posisjon» lett kan forseres og vil medføre en økt sårbarhet. Vinduer og dører som er nært bakkeplan bør ha samme sikkerhetsnivå som ytterdøren.
- Gjør deg kjent med beskyttelsesnivået som du har på dører og vinduer.
- Monter og benytt sikkerhetslås på døren ved behov.
- Monter et kikkhull eller ringeklokkekamera. Se alltid etter hvem som befinner seg på yttersiden før du åpner døren.
- Vinduene kan sikres ytterligere ved å montere spesialfolie eller gitter. Det vil ofte gi en bedre beskyttelse mot inntrengning.

Nøkler, kort, brikker og koder

- Ha kontroll på alle nøkler, brikker, adgangskort og portnøkler. Sørg for at disse ikke kan identifiseres hvis de kommer på avveie. Bytt adgangskoder når det er nødvendig.
- Dersom du mister et digitalt nøkkelkort eller brikke på offentlig sted skal du som hovedregel erstatte dette med et nytt selv om du gjenfinner det senere.

Boligalarm

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



Din egen bolig er et sted der potensielle trusselaktører kan oppsøke deg

Trygge rom

- Identifiser det tryggeste rommet i boligen din. Dette kan for eksempel være et rom som er mulig å låse og hvor det ikke er et vindu. Sørg for at du har mobildekning inne på rommet eller at det er andre måter å kommunisere derfra på.

Anonymiser boligen

- Unngå å ha navnet ditt på ringeklokken og døren.
- Unngå å legge ut detaljer og bilder fra boligen din på sosiale medier og ellers på nett. Det kan utnyttes av en potensiell trusselaktør. Det samme gjelder informasjon som du gir i intervjuer som kan bidra til å identifisere hvor du bor, eller området du bor i.

Innsyn

- Vær bevisst på hvorfra det eventuelt er innsyn, både ute og inne.
- Bruk eventuelt gardiner, persienner eller annen skjerming. Hekk, mur, levegger og gjerder rundt uteområder kan ha god skjermingseffekt.
- Utendørs sittegrupper og lignende bør plasseres med tanke på at de både ivaretar behovet for skjerming mot innsyn og på samme tid ivaretar muligheten for at du raskt skal kunne trekke inn i boligen din ved behov.

Grenser og barrierer

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

Skjerming av kjøretøy

- Parker om mulig bilen din i en egen garasje, på egen eiendom og helst slik at registreringsnummeret ikke er synlig fra offentlig sted.
- Unngå å bruke samme gateparkering over tid.

2.4 | Tradisjonelle og sosiale medier

For de som er politisk aktive så er det viktig å nå ut til ulike målgrupper, blant annet gjennom aktiv bruk av både tradisjonelle og sosiale medier. Sosiale medier følges av enkeltpersoner og av de tradisjonelle mediene, og det er ofte stor interesse for politikeres digitale tilstedeværelse. Imidlertid kan eksponering i ulike medier føre til uønskede sårbarheter for deg,

ditt virke og for andre. Opplysninger om familie, venner, hvem du omgås, samt faste rutinepregede aktiviteter kan utnyttes i en eventuell kartlegging av deg. Privat og sensitiv informasjon kan misbrukes og benyttes til å forsterke trusler eller anvendes i et utpressingsøyemed. Det samme kan også gjelde for informasjon om virksomheter og steder som du besøker.

Veileder for sosiale medier

Vær kritisk

- Vær oppmerksom på at profiler og informasjon i sosiale medier kan være falske.
- Henvendelser og lenker du mottar i ulike sosiale medier og meldingsapper kan være forsøk på cyberangrep.
- Gjør en kritisk vurdering før du installerer nye apper og ha restriktive personverninnstillinger i alle sosiale medier og øvrige apper.

Begrens eksponering av oppholdssteder og vaner

- Adskill offentlige og private profiler på sosiale medier.
- Det er greit å være personlig, men unngå å være 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, handle, hvor barna dine går i barnehage, på skole, hvor du skal reise på ferie eller informasjon om andre steder som 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 eller at du har reist der ifra.
- Vær oppmerksom på at familiemedlemmer eller andre likevel kan eksponere det som du selv ønsker å skjerme. Ta derfor en samtale om bruken av sosiale medier med dem som står deg nær.

Eksponering i ulike medier kan føre til uønskede sårbarheter.

Kontroller og moderer

- Dersom du har en offisiell side på sosiale medier bør det etableres klare retningslinjer for hvordan trusler og hatefylte ytringer skal håndteres. Det kan i de fleste tilfeller være hensiktsmessig at sosiale medier administreres av noen i ditt støtteapparat.
- Dersom du opplever ytringer i sosiale medier som påvirker deg negativt, så 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:

- Du mottar e-poster eller meldinger som er målrettet mot deg og som er mistenkelige eller uvanlige.
- Noen misbruker dine profiler eller bilder i sosiale medier.
- Noen sprer falsk informasjon om deg eller dine nærmeste som kan påvirke din sikkerhet.

Ved potensielt straffbare ytringer, for eksempel trusler:

- Ta skjermdump eller bilde av innlegget og profilen som publiserte det. Få med informasjon om tidspunkt, plattform, avsender og annet som kan beskrive sammenhengen. Meld fra både til egen (parti)organisasjon/ virksomhet og til PST eller politiet.

Håndtering av trusler på telefon

Du og dine nærmeste kan motta alvorlige trusler på telefon eller talemeldinger på apper. I disse tilfellene bør du:

- Avbryte samtalen og avvise nye oppringinger fra samme person.
- I noen tilfeller kan det være aktuelt å ta opp lyd fra samtalen eller skru på høyttaleren så andre også kan høre samtalen.
- Forsøk å legge merke til vedkommendes alder, navn, dialekt, bakgrunnsstøy, telefonnummer.
- Meld fra både til egen (parti)organisasjon/virksomhet og til PST eller politiet.



2.5 | Håndtering av fysiske trusler og angrep

Som myndighetsperson bør du være forberedt på at en uønsket eller truende hendelse kan inntreffe. Det er derfor fornuftig at du på forhånd ser for deg noen alvorlige scenarioer som kan oppstå og forbereder deg, og de rundt deg på hvordan du/dere kan handle i slike situasjoner. Du bør se for deg og forberede deg

på scenarioer som kan oppstå i situasjoner som for eksempel offentlige opptredener, på arbeidsplassen, på reise eller i tilknytning til hjemmet ditt. En slik mental forberedelse kan i noen tilfeller være avgjørende for å redusere konsekvensene.

Håndtering akutte situasjoner

Dersom du opplever å bli truet

- Prøv å opptre rolig.
- Føler du deg truet, så skal du varsle. Ikke vent med å få en mulig truende situasjon bekreftet.
- Utløs alarm eller varsle politiet på 112.
- Formidle hvordan trusselen blir formulert og hva vedkommende sier.
- Si tydelig ifra til den som trækker over grensene dine som for eksempel «dette er truende – gå bort!».
- Gjør fysisk motstand dersom du må.

Ved bopel

- Trekk inn i boligen og lås vinduer og dører.
- Gå til sikkert rom.

På offentlig sted

- Unngå en direkte konfrontasjon og trekk deg unna.
- Oppsøk et sted hvor det er andre personer eller tilkall oppmerksomhet og be om hjelp.

2.6 | Terrorangrep og andre alvorlige voldsscenarioer

Selv om det er svært lite sannsynlighet for at du kan bli utsatt for et terrorangrep så kan kunnskap om slike situasjoner redde livet ditt. Dette er uavhengig av om angrepet skulle skje i Norge eller et sted i utlandet. En måte å være mentalt forberedt på er å forsøke å forestille seg noen ulike scenarioer og situasjoner som kan forekomme og finne frem til ulike måter som du ville handlet på. Det vil trolig være kort tid fra du inn-

ser hva som er i ferd med å skje, til at du må handle. Ved en forhøyet terrortrussel så bør du være særlig oppmerksom når du befinner deg på steder som sikkerhetskontroller, inngangspartier eller utenfor potensielle angrepsmål. Gjør deg derfor kjent med rømningsveiene på hoteller, i bygninger og på offentlige steder som du oppholder deg, selv om det er for korte tidsrom.

Handling ved terrorangrep og andre alvorlige voldsscenarioer

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

1. Flykt

- Forsøk å lokalisere hvor terroristene befinner seg og flykt i en annen retning. Ikke ta med deg unødvendige gjenstander. Forsøk å advare andre om faren.
- Dersom terrorangrepet startet med en eksplosjon så må du i tillegg være oppmerksom på at det kan være andre farer som branner, gasslekkasjer, usikrede strømledninger og ustabile bygninger.
- Vær forberedt på at det kan komme ytterligere angrep, for eksempel fra andre bevæpnede terrorister eller eksplosjoner.
- Ved et kjøretøyangrep så flykt på tvers av bilens kjøreretning.

2. Søk dekning

- Dersom det ikke er mulig å rømme så bør du finne deg et sikkert gjemmested som kan låses eller barrikaderes.
- Lås døren, slukk lyset, begrens innsyn og vær stille. Hold deg unna vinduer og dører til du er helt sikker på at faren er over.
- Skru av all lyd og vibrering på mobilen og skru også ned lysstyrken på skjermen for ikke å avsløre hvor du er.
- Ikke ring unødvendig til personer som fremdeles kan befinne seg inne i risikoområdet. Det kan utsette dem for unødvendig fare.



- Vær bevisst på at skjul og dekning ikke alltid er det samme. Det betyr at selv om en terrorist ikke kan se deg, så kan du i likevel bli rammet av prosjektiler. Søk derfor helst dekning bak solide vegger av mur, stein eller lignende.

3. Varsle

- Varsle politiet så raskt som mulig. Fortelle hvem det er som ringer, hvor du ringer fra og fortell hva som skjer.
- Hvis du ikke kan snakke så kan du skru av lyden, men likevel ha en åpen linje på telefonen slik at politiet kan lytte til hva som skjer rundt deg.
- Følg politiets anvisninger og besvar spørsmål.
- Husk at du kan ha viktig informasjon som kan gi politiet bedre forutsetninger for å kunne stanse angrepet.

Dersom du ikke har noe annet valg og det står om liv, så angrip gjerningspersonen med alle tilgjengelige hjelpemidler.

Når politiet eller sikkerhetspersonell ankommer så er det viktig at du opptrer rolig og at du ikke handler på en måte som kan oppfattes som at du er en av gjerningspersonene. Ikke hold gjenstander i hendene og hold hendene godt synlig for politiet. Vær forberedt på at du kan bli pekt på med skytevåpen og bli gitt ordre av politiet i den akutte fasen. Gjør som du får beskjed om. Politiet vil prioritere å stoppe gjerningspersonene og avverge at nye skader oppstår. Eventuell førstehjelp vil kunne måtte vente.



3

Sjikane, hets og trusler

Konkrete trusler, men også et stort omfang av fiendtlige og negative personrettede ytringer kan få store konsekvenser for deg som myndighetsperson og for dine nærmeste. Et økende omfang av hets, sjikane og trusler kan føre til at enkelte politikere velger å trekke seg fra den offentlige debatten. I verste fall kan noen velge å avstå fra å stille til valg og drive politisk arbeid.

Hets, sjikane og trusler fremsettes hovedsakelig i kommentarfelt og i sosiale medier på internett. De som står bak dem er som oftest drevet av en personlig motivasjon og/eller er i en vanskelig livssituasjon. En fellesnevner for disse personene er at de i ulik grad er myndighetsfiendtlige.

Ytringene knyttes ofte til politiske enkeltsaker, partitilhørighet eller er generell «trolling». De færreste som fremsetter denne typen trusler gjennomfører voldshandlingene de truer med.

Enkle tiltak kan redusere sannsynligheten for at du mottar denne typen uønskede ytringer. Disse består oftest i å redusere tilgangen til deg og dine nærmeste, ikke minst tilgjengeligheten på sosiale medier og på internett for øvrig.

Alle myndighetspersoner og politikere må likevel være forberedt på at det tidvis kan være et tøft og ubehagelig debattklima og et stort personfokus. Et viktig mål med forebyggende sikkerhetstiltak er likevel å redusere

den negative virkningen av sjikane, hets og trusler. De som mottar trusler, får ofte en tilleggsbelastning ved at de opplever å bli stående alene i håndteringen og konsekvensene. Slik trenger det ikke å være. Det er derfor viktig at du involverer lederen din, (parti)organisasjonen eller virksomheten din tidlig. Gode rammer, rutiner og tiltaksplaner for å håndtere denne typen hendelser gjør deg som myndighetsperson mer robust. Det er et felles ansvar å samle seg rundt og støtte de som utsettes for hets, sjikane og trusler.

3.1 | Forebyggende råd

- Skjerm deg fra unødvendig informasjon.
- Forum og kommentarfelt inneholder ofte personrettet sjikane eller trusler. Monitorering av slike arenaer kan over tid være unødvendig belastende for deg. I den grad det er nødvendig å følge med på dette, så kan det være hensiktsmessig at det er andre enn deg selv som gjør det.
- Sjikane og trusler skal ikke tolereres, så sett tydelige grenser. Avslutt samtaler eller diskusjoner som utvikler seg i en negativ retning. Dette kan forebygge at det kommer mer alvorlige trusler. Blokker og rapporter personer/profiler som opptrer uakseptabelt.
- Reserver deg mot nummeropplysningstjenester. Slik skjerming vil gjøre deg mindre tilgjengelig, særlig for mer spontane henvendelser. Familiemedlemmer eller andre beboere med kjent tilknytning til deg bør også skjermes. Vurder også om du trenger å ha kontaktinformasjon din tilgjengelig på hjemmesiden til virksomheten eller partiet.

3.2 | 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, men du bør likevel ta dem på alvor. Ha en plan for håndtering av slike hendelser, og følg den.

Del informasjonen med andre

- Involver din egen (parti)organisasjon/virksomhet, leder eller sikkerhetsansvarlig. Organisasjonen eller virksomheten har et ansvar og de bør ha gode rutiner for håndtering av slike hendelser. Deres mulighet til å hjelpe deg avhenger av at du informerer dem om skulle skje.

Bearbeid inntrykk og følelser, gjerne sammen med andre

- Trusler eller omfattende negativt personfokus kan utgjøre en stor personlig belastning, også for dine nærmeste. Det er derfor viktig at dere snakker om slike opplevelser.
- Hvis du opplever at du innskrenker aktivitetene dine, begrenser ytringene dine, føler frykt eller får helseplager så er det viktig at du oppsøke støtte og hjelp. Det er viktig at politiske partier og virksomheter tilrettelegger for slike samtaler. Dersom du er åpen om dine opplevelser og følelser så kan det også motivere og senke terskelen for andre til å åpne seg om sine opplevelser.

3.3 | Varsling av trusler til myndighetene

Trakassering, trusler og vold kan inntreffe til tross for at det er igangsatt forebyggende tiltak. Det er viktig at du rapporterer alvorlige og straffbare trusler til politiet. Selv om du er usikker på grensen så bør du likevel ta kontakt med politiet eller PST for at de kan gjøre en nærmere vurdering av alvorligheten. Informer også internt i virksomheten din eller (parti) organisasjonen, samt din nærmeste leder.

Avhengig av hvem trusselen er rettet mot og hva som er motivet bak trusselen, så er det enten PST eller politiet som håndterer denne typen saker. Dersom det fremsettes trusler mot myndighetspersoner og trusselen kan knyttes til din rolle og posisjon så er det i utgangspunktet PST som har ansvaret for å etterforske saken. PST og politiet kan vurdere å øke sikkerhetstiltakene på bakgrunn av mottatte trusler, uavhengig av om saken etterforskes eller ikke. Det er derfor viktig at du varsler en gang for mye enn en gang for lite.

Varsling om trusler

- Hvis det er fare for liv og helse, så bør du utløse alarmen eller ringe politiets nødnummer 112.
- Ved andre straffbare forhold eller bekymringer så ring lokalt politi på 02800.
- Trusler mot myndighetspersoner som ikke er akutte varsles i etablerte kanaler eller til PSTs døgnåpne responscenter: 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 kan være relevant for PST og politiet.

3.4 | Håndtering av trusler eller andre potensielle sikkerhetstruende henvendelser

Fremsatte trusler bør sikres både av hensyn til etterforskning og for at de skal kunne vurderes og håndteres av andre, som PST eller politiet.

Du kan sikre digitalt fremsatte trusler ved å ta skjermbilde av dem, sørg for å få med plattform og tidspunkt. Om mulig er det en fordel om du kan sikre et skjermbilde av avsenderens profil og gjerne en lenke til profilen siden kontekst er viktig. Ta gjerne flere skjermbilder og

forsøk å gi utfyllende informasjon, for eksempel om bakgrunnen eller rammene for hendelsen.

Av og til mottar myndighetspersoner fysiske trusselbrev. Disse bør tas på av så få personer som mulig ta gjerne et foto av det og oppbevar det for eksempel i en papir- eller plastpose. Ta kontakt med politiet for videre oppfølging og råd.





4

Informasjons- sikkerhet

Norge og norske interesser står overfor en vedvarende etterretnings-trussel fra fremmede stater. Deres formål er å innhente informasjon om norske politiske prosesser, forsvar, beredskap og teknologi. Myndighetspersoner og politikere på alle nivåer er derfor viktige barrierer i arbeidet med å beskytte samfunnskritiske verdier.

4.1 | Etterretningstrusselen

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

Husk at det ikke nødvendigvis er myndighetspersonen selv som blir kontaktet i disse sammenhengene. Det kan også være at noen i støtteapparatet ditt vil være et mål for etterretningsaktivitet. Disse vil i stor grad ha tilgang til mye av den samme informasjonen som deg og kan også fungere som en potensiell «bro» videre mot et annet mål. Vær derfor ekstra oppmerksom og bruk sunn fornuft om du tror at du blir kontaktet av representanter fra fremmede stater, spesielt fra dem som PST, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet advarer mot i de nasjonale trusselvurderingene. Opplever du mistenkelige henvendelser eller tilnærmelser må du varsle PST og eventuelt din egen sikkerhetsorganisasjon så snart som mulig.

Cyberangrep er en mye brukt metode for spionasje. Dette kan forløpe på mange forskjellige måter og fra ulike innfallsvinkler. Teknologien som brukes til å utføre angrepene utvikles kontinuerlig. Etterretningsverdig informasjon blir ofte lagret digitalt. Privat og sensitiv informasjon som bilder og meldingslogger kan også brukes til utpressing eller påvirkning av beslutninger hvis de kommer på avveie. Det er derfor viktig at du følger oppdaterte sikkerhetsrutiner og råd for cybersikkerhet.

Mange av rådene som forebygger generell kriminalitet har også stor overføringsverdi til å forebygge etterretningsvirksomhet. Er du flink til å beskytte viktig og sensitiv informasjon så reduseres også sannsynligheten for at noen stjeler og bruker informasjonen din på uønskede måter mot deg selv eller andre.

Råd som kan forebygge ulovlig etterretning

Ved reiser til steder med forhøyet etterretningstrussel se punkt 5.3.

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 verdien av den.

Skap en sikkerhetskultur

- Ha hele tiden 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, så bør du følge det opp. Vær oppmerksom på personer som utviser påfallende stor interesse for deg som person, (parti) organisasjonen/virksomheten eller arrangementer, eller som snakker med deg om andre personer.
- Er du i tvil så bør du varsle PST, politiet eller egen organisasjon/virksomhet.

Verifiser dem som tar kontakt med deg

- Dagens teknologi muliggjør det å utgi seg for å være noen andre på en troverdig måte. Inkludert personer og virksomheter som du kjenner til fra før av, både via meldinger, video og på telefon. Ikke åpne vedlegg eller lenker dersom du synes noe virker rart.
- Er du i tvil, så kan du for eksempel verifisere at noen er den de utgir seg for ved å ringe dem tilbake via et sentralbord dersom det er mulig



4.2 | IKT-utstyr og internettsikkerhet

De gjeldende rådene for digital sikkerhet endrer seg raskt. Nasjonal sikkerhetsmyndighet (NSM) er ansvarlig for nasjonale digitale sikkerhetsråd. NSMs råd er i stor grad rettet mot virksomheter og i mange tilfeller er det derfor mest riktig å henvise spørsmål om digital sikkerhet til egen sikkerhetsorganisasjon i første rekke. Til tross for den raske utviklingen på området så er det imidlertid noen overordnede råd som vil være gyldige selv over tid.

Selv om rådene i stor grad gjelder digital sikkerhet så er det viktig også å ha kontroll på sensitive dokumenter, samt å være oppmerksom på at dine samtaler også kan fanges opp av andre. 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 og lignende i rommet.
- Skill tydelig mellom privat og jobb i sosiale medier, der du lagrer data, og i forbindelse med elektronisk kommunikasjon. Krypterte kommunikasjonsapplikasjoner er ofte mindre sårbare enn SMS og e-post.
- Bruk VPN da den vil bidra til å skjule datatrafikken din for uvedkommende. For private enheter bør du alltid velge en pålitelig VPN-leverandør. For tjenesteenheter vil det som regel være organisasjonen/ virksomheten din som setter opp VPN. Ved reiser må du være oppmerksom på at enkelte land ikke tillater eller har sterke begrensninger på bruk av VPN.
- Ikke åpne vedlegg, lenker eller QR-koder som du ikke er helt sikker på. Du kan også kontakte avsenderen 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. Banker og myndigheter vil aldri spørre om slik informasjon.
- Ha fysisk kontroll på mobiler og annet digitalt utstyr og ikke lån dem bort til andre.
- Forsøk å lage sterke passord og lag ulike passord til hver tjeneste.

Trådløst internett

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

-
- Bruk flerfaktor-autentisering der det er mulig (passord i kombinasjon med finger- eller ansikts-gjenkjenning, kodebrikke eller lignende).
 - Ikke bruk USB-ladere på kollektivtransport, flyplasser og hoteller. Ved lading så bruk en USB-overgang som blokkerer for dataoverføring, egen bærbar powerbank eller bruk en ordinær lader med støpsel.
 - Ikke bruk, lån av andre eller la andre låne USB-enheter, USB-kabler eller minnekort.
 - Oppdater alltid antivirusprogrammer, operativsystemer og apper med siste versjon av programvaren og skru på automatiske oppdateringer der det er mulig.
 - Eldre mobiler får ikke alltid siste sikkerhetsoppdateringer. Det er derfor viktig å bytte ut eldre utstyr dersom leverandøren slutter å tilby slike oppdateringer.
 - Krypter harddisker og lignende lagringsmedier.
 - Gjør en kritisk vurdering av apper før installering. Vær også 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 | Sikker håndtering av mobiler

Mobil teknologi gjør det mye enklere å være tilgjengelig i dagens teknologiske samfunn. Samtidig er det viktig å være bevisst på ulike sårbarheter som kan eksponere innholdet på din mobil eller i digitale skyer. Mobiler og brukerkontoer genererer og lagrer svært mye informasjon som kan havne i kommersielle databaser. Informasjon selges ofte videre og

det finnes måter for en trusselaktør å gjøre at slik anonymisert informasjon likevel blir tilgjengelig for dem. Mange apper lagrer posisjonsdata i ulike situasjoner, noe som kan hentes frem av uvedkommende. Det er derfor viktig å være kritisk til hvilke funksjoner du slår på og bruker på mobiltelefoner og nettbrett.

Sikkerhetsråd for mobiltelefoner og nettbrett

- Gjør deg kjent med de gjeldende reglene 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 for fjernsletting av 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 som du får på SMS, e-post eller tilsvarende.
- Skru av blåtann, trådløst nett og andre overføringsmuligheter når de ikke benyttes. Sørg for at kun godkjente kontakter kan sende noe til deg via AirDrop eller tilsvarende.
- Vurder nødvendigheten av skylagring eller digitale sikkerhetskopier. Disse kan bli tilgjengelige for andre via fjerntilgang.
- Slett sensitiv historikk for anrop, e-post, SMS og kontaktlister jevnlig. Dette kan eksterne aktører få tilgang til.
- Slett alt innholdet på mobilen før du leverer den til service eller bytter den inn. For tjenesteenheter må du følge de reglene din organisasjon eller virksomhet har for service eller reparasjoner.
- Vær oppmerksom på om mobilen får avvikende adferd eller ytelse. Eksempler på dette kan være at den bruker uforholdsmessig mye data, minne, 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 om du skal varsle myndighetene.

4.4 | Varsling

Det er viktig å ha lav terskel for å varsle om mistenkelig eller uvanlig aktivitet som kan være relatert til etterretningsaktivitet og infor-

masjonssikkerhet. Graden av ditt behov for hjelp vil være avgjørende for hvem som du bør kontakte.

Pågående datainnbrudd

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

Ved mistanke om at noe er galt

- Har du indikasjoner på at noe er galt med tanke på digital sikkerhet så bør du først og fremst varsle de som administrerer utstyret ditt.
- Fremstår det som et lovbrudd, så bør politiet varsles og forholdet anmeldes.

Mistenkelig tilnærming

- Hvis du mistenker at utenlandsk etterretning kontakter deg på elektroniske medier, eller om du opplever at noen utviser påfallende stor interesse for deg og ditt virke så bør du drøfte dette med en ansvarlig i egen (parti)organisasjon eller virksomhet, og deretter varsle PST.
- PST kan gi spesifikke råd ut fra en vurdering av situasjonen hvis du er usikker.



5

Sikkerhet på reise

Ved reiser til utlandet kan du komme i situasjoner der din eller andres sikkerhet blir truet. Det finnes mange måter du kan oppnå bedre sikkerhet på, men en av de viktigste er å gjøre gode forberedelser før reisen starter.

5.1 | Ordinære reiser

Vurderinger av sikkerhetstiltak

bør inngå i all planlegging av reiser og spesielt dersom reisen er til områder med økt risiko. På utenlandsreiser kan trusler og sårbarheter knyttet til høy kriminalitet, terrorisme, kidnapping, naturkatastrofer, trafikksikkerhet, infrastruktur, helseutfordringer og etterretningsvirksomhet være svært aktuelle. Trusselbildet for ulike regioner, land og områder kan være forskjellig. En sikkerhets-situasjon kan endre seg raskt og bli utrygg og uforutsigbar uten forvarsel.

På Utenriksdepartementets (UD) nettsider kan du finne viktige opplysninger om sikkerhetssituasjonen i det landet du skal reise til. UD tilbyr også reiseregistering, hvor du legger inn informasjon om den forestående reisen og kontakthinformatjonen din. Dette gjør at norske myndigheter enklere kan ha oversikt over alle reisende som oppholder seg i et gitt land og dermed komme raskere i kontakt med dem. Dette kan være av stor betydning ved for eksempel varsling av ekstraordinære hendelser som naturkatastrofer.

Før avreise

- Det anbefales at det utpekes en person som er ansvarlig for å vurdere om risikoen på reisen er akseptabel. Dersom den ikke er det så bør det vurderes om det skal settes på flere risikoreduserende tiltak eller om reisen skal utsettes eller avlyses i sin helhet.
- Det anbefales videre at det utpekes en person som er ansvarlig for gjennomføringen av reisen. Vedkommende kan for eksempel kunne:
 - Lage en oversikt over nødvendige vaksiner
 - Etablere kontakt med den norske ambassaden
 - Innhente beredskapsplaner hvis det er utarbeidet for reisen eller destinasjonen.
 - Vurdere helsesituasjonen og brannsikkerheten
 - Lage en liste med viktige telefonnummer i besøkslandet
 - Utpeke felles samlingssteder ved uforutsette hendelser
 - Kartlegge ulike transportmidler under oppholdet
 - Opprette en kryptert chat for reisefølget i tråd med virksomhetens rutiner
 - Fungere som kontaktpunkt og koordinator på reiser med mange deltagere
- Alle reisende bør uavhengig av dette sette seg inn i situasjonen i det området som dere skal besøke.
- Tenk gjennom hvilke uønskede hendelser som kan skje og hvordan du vil løse dem.
- Ta med deg gyldige reisedokumenter og nødvendig utstyr. For eksempel enkelt førstehjelpsutstyr, reiseapotek, bærbar powerbank, strømadapter, lommelykt og kontanter.
- Innhent viktige telefonnummer som for eksempel til den norske ambassaden, lokalt politi og nød nummer, norske myndigheter og lagre disse på mobilen.
- Ta i tillegg med en fysisk kopi av pass, kredittkort, reisedokumenter og nødvendig kontaktinformasjon (i tilfelle du mister mobilen din).
- Sørg for å ha en reiseforsikring som gjelder for besøkslandet og den aktiviteten som du skal utføre.
- Selv om dere er flere som reiser sammen, så fritar ikke det hver enkelt fra et felles ansvar for sikkerheten. Ser du noe, så si noe.

Sikkerhetsråd under transport og i transitt

- Opphold deg kortest mulig tid i avgangshallen før du går gjennom sikkerhetskontrollen til et mer sikkert område.
- Ha alltid kontroll på din egen bagasje og sjekk om noen har åpnet eller forsøkt å åpne den.
- Tyverier skjer ofte under transport og gjerne på flyplasser, ved inn- og utlasting av kjøretøy og på spisesteder.
- Hvis mulig så hold deg sammen med reisefølget ditt.
- Vær presis ved oppmøte til avtaler og transport.
- Unngå å sette deg i situasjoner der din vurderingsevne blir vesentlig redusert for eksempel ved bruk av rusmidler.
- Undersøk hvilke transportmidler det er anbefalt å benytte i det aktuelle området.
- Hold dører og vinduer lukket og låst under transport i bil.

På hotellet

- Etter ankomst på hotellet bør du gjøre deg kjent med hotellets sikkerhetsrutiner og nødutganger.
- Om mulig, så samle reisefølget slik at alle bor i samme etasje og helst i nærheten av hverandre. Be om at rommene deres ikke er på bakkeplan, men fortrinnsvis mellom 3. til 6. etasje, og helst ikke plassert direkte over resepsjonen.
- Ha oversikt over hvor alle de andre i reisefølget ditt bor.
- Avtal et sikkert sted der reisefølget skal møte dersom det oppstår en uforutsett hendelse. Det kan være det mest egnede rommet dere har, et bomberom eller utendørs, men unngå resepsjonen.
- Lås alltid døren og bruk alltid sikkerhetslenken når du er inne på hotellrommet.
- Vær oppmerksom på at hotellrom, møterom, fasttelefon og mobil kan bli avlyttet. Skjult videoovervåking av rommene kan også forekomme.
- Unngå å legge igjen sensitive dokumenter og elektroniske enheter på hotellrommet ubevoktet.
- Sett opp egen røykvarsler beregnet for reiser, dersom det ikke allerede er røykvarsler på rommet.
- Vurder å bytte rom, etasje eller hotell dersom du føler deg utrygg.

I det offentlige rom

- Vær alltid oppmerksom på omgivelsene dine. Dersom du føler at du er utrygg så oppsøk hjelp eller gå inn på et trygt sted som for eksempel et hotell, politistasjon eller lignende.
- Vis alltid respekt for kulturen, religion og tradisjonene i landet som du besøker.
- Sørg for å vite hvor du befinner deg til enhver tid og noter deg navnet og adressen på hotellet ditt.
- Om du må forlate reisefølget ditt så meld ifra hvor du skal og når du planlegger å være tilbake. Informer også om hvordan de kan komme i kontakt med deg.
- Situasjoner som senere kan brukes som et pressmiddel mot deg kan bli fremprovosert. Om dere er flere sammen så reduseres muligheten for å bli utsatt for denne typen hendelser.
- Dersom du opplever ubehagelig tilnærming av politi, sikkerhetspersonell eller tilsvarende, må du likevel opptre korrekt. Forsøk å unngå å bli dratt inn i en vanskelig situasjon.
- Tenk over hva du sier, og hvor du sier det. Uvedkommende kan lytte på samtalen og du kan være under observasjon. Ikke la andre få innsyn til hva du jobber med på PC og nettbrett.
- Lokalt ansatte ved norske virksomheter i utlandet kan bli utnyttet eller bli brukt som informanter. Vær derfor bevisst på hva du deler med dem og hva du snakker om i deres nærvær.
- Uønskede hendelser bør rapporteres til norske myndigheter.
- Pass på tingene dine.
- Ha alltid mobiltelefonen med deg.
- Unngå å oppsøke områder og situasjoner som kan utvikle seg til å bli truende (kriminalitet, demonstrasjoner og opptøyer).
- Unngå å tiltrekke deg unødvendig oppmerksomhet fra kriminelle. Vis aldri frem penger eller verdisaker. Synlige lapper med navn, telefonnummer og adresse utenpå bagasjen kan utnyttes av kriminelle. Ta hensyn til det når du merker bagasjen din.



5.2 | Reiser til steder med forhøyet risiko

Noen reiser krever ekstra forberedelse og en høyere beredskap for uønskede hendelser. Det kan være flere kjente grunner til dette, som høy terrortrussel, svært høy kriminalitet, manglende evakueringsmuligheter eller begrensende muligheter for medisinsk behandling. I de fleste tilfeller vil PST gjøre en risikovurdering av reisen dersom en myndighetsperson i embetsmedfør, reiser til et land med et skjerpet trusselbilde. Ofte vil det da bli iverksatt risikoreduserende tiltak og gitt sikkerhetsrådgivning i forkant av reisen.

En av de beste risikoreduserende tiltakene ved reiser til steder med høy risiko er å ha kontroll på informasjonen om reisen. Vær derfor varsom med hvem som du deler informasjon om den kommende reisen med. I hovedsak bør færrest mulig ha kjennskap til at reisen skal gjennomføres og sikkerhetstiltakene bør skjermes spesielt.

Sikkerhetsrådene som er nevnt tidligere gjelder også for reiser til risikoutsatte områder. I tillegg bør rådene i de følgende punktene etterfølges

Før reiser til steder med forhøyet risiko

- Avklar hvem som er leder på reisen og hvem som bør godkjenne risikoen forbundet med reisen. De to rollene bør ikke innehas av samme person.
- Innhent god og tidsaktuell informasjon om sikkerhetssituasjonen i området du skal besøke.
- Informer relevante myndigheter, som PST og Utenriksdepartementet om den forestående reisen i god tid før avreise.
- Gjennomfør et planleggingsmøte hvor behovet for konkrete sikkerhetstiltak og utstyr vurderes.
- Sørg for at alle som skal delta på reisen deler den samme forståelsen av risikobildet.
- Vurder om du skal ha med en satellitttelefon.
- Ta med en reiseveske (grab-bag) med nødvendig utstyr som til enhver tid er ferdigpakket og lett tilgjengelig i tilfelle evakuering. Du bør alltid ha vesken med deg siden det ofte er vanskelig å forutsi når du vil få behov for den. Vesken bør inneholde førstehjelpsutstyr, hodelykt, vann, lettere proviant, pass, kredittkort, ekstra klær og en bok eller annet tidsfordriv. Dersom det er aktuelt så bør du også ta med eventuelle sensitive dokumenter, utlevert sikkerhetsutstyr og eventuelle medisiner som du bruker til daglig. Forsøk likevel å unngå å ta med deg for mange unødvendige gjenstander.

Under reise og transport til steder med forhøyet risiko

- På reiser er det som oftest transportetappene som er mest risikoutsatt.
- Vær oppmerksom på omgivelsene dine. Begrens bruken av hode-telefoner/øreplugg. Det kan forhindre deg fra å oppfatte viktige meldinger eller oppfatte truende situasjoner.
- Vent innendørs til alle er til stede og transporten er klar.
- Hold dører og vinduer lukket og låst under transport.
- Hold deg oppdatert på sikkerhetssituasjonen og vær forberedt på at den kan endre seg raskt.
- Følg med på lokale og internasjonale nyheter.
- Ved ekstraordinære hendelser så bør du følge instruksene fra sikkerhetspersonellet og lokale myndigheter.
- Bruk utlevert sikkerhetsutstyr dersom du får beskjed om det (vernevest, hjelm o.l.).

På hotellet

- Om mulig så bør du gjøre deg kjent med og gå evakueringsruten for å se at den er fremkommelig. Vær oppmerksom på at enkelte dører kan være alarmbelagt.
- Merk deg plasseringen av tilfluktsrom eller sikre rom.
- Sjekk telefonforbindelsen hjem, til andre i reisefølget og til hotellets resepsjon.
- Ikke gi fra deg eller på annen måte eksponer romnummeret ditt for uvedkommende. Husk at romnummeret kan stå på nøkkelen eller på papiromslaget. Oppbevar omslaget og nøkkelkort hver for seg.
- Begrens innsynet til hotellrommet.

I det offentlige rom på steder med forhøyet risiko

- Unngå opphold i det offentlige rom så langt som mulig.
- Følg med på omgivelsene rundt deg og planlegg hvordan du eventuelt kan trekke deg unna dersom en truende situasjon skulle oppstå.
- Respekter eventuelle pålagte begrensninger i din bevegelsesfrihet og opphold deg i hovedsak på området som er definert som trygt, som for eksempel på hotellet.
- Gå alltid 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 lettere kan gli inn i folkemengden. Prøv å ikke se verken «militær» eller velstående ut. Dette kan øke den negative oppmerksomheten rundt deg.
- Plasser deg slik at du har en god oversikt der du til enhver tid befinner deg, som i restaurantlokalet, på et tog, i en folkemengde osv.
- Kartlegg hvor de til enhver tid nærmeste nødutgangene befinner seg.

Etter reisen til steder med forhøyet risiko

- Hvis det har oppstått sikkerhetstruende eller problematiske situasjoner under reisen så informer om dette til (parti)organisasjonen eller virksomheten din. Vurder om du skal gjøre det umiddelbart eller etter hjemkomst. Vurder videre om du også skal informere PST om hendelsene.
- Husk at dine opplevelser og erfaringer kan være nyttig informasjon for de som skal vurdere risikoen på reiser til samme sted senere.

Truende situasjoner

- Følg godt med på dine omgivelser og forsøk å unngå å bevege deg inn i en situasjon som kan utvikle seg til å bli truende.
- Dersom du befinner deg i en truende situasjon så forsøk å komme deg bort fra den og oppsøk et tryggere sted.
- Hvis du ikke kan komme deg unna situasjonen, så påkall andres oppmerksomhet.
- Adlyd de ordrene som du blir gitt. Det er bedre å gi fra deg lommebok, veske eller andre verdigjenstander enn å holde disse tilbake.
- Hvis du blir utsatt for en truende hendelse, som for eksempel provokasjon, forulemping, fysisk angrep, ran eller gisseltaking så vil dine egne reaksjoner være avgjørende for både deg selv og de du er sammen med.
- Behold roen, vær høflig og opptre korrekt. Reaksjonsformen din må stå forhold til trusselens alvorlighet og den konkrete situasjonen. Dette kan påvirke gjerningspersonen i positiv retning.
- Gjør motstand bare dersom du må.

Flykt – Søk dekning – Varsle



Spesielt om gisselsituasjoner

- Gjør som du får beskjed om.
- Gisseltakerne er også stresset og de kan anse deg som en trussel.
- Forvent røff behandling, mye støy og en uoversiktlig situasjon.
- Forsøk å bevare roen, snakk rolig og tydelig. Svar på eventuelle spørsmål som du blir stilt.
- Forsøk å varsle norske myndigheter eller andre om at du har blitt tilbakeholdt så raskt som mulig.
- 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 mens du er i fangenskap, også elektronisk.
- Selv om det vil bli iverksatt et stort apparat for å hjelpe deg, så må du selv aktivt forsøke å forbedre din egen situasjon.

Terrorangrep eller livstruende situasjoner

I enkelte land, regioner og byer er det høyere risiko for et 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 du kommer deg uskadet fra en livstruende situasjon. Dersom du ledsages av sikkerhetspersonell så må du følge deres råd og ordrer uten opphold.¹

1) Se punkt 2.6 for mer informasjon om terrorangrep

5.3 | Informasjonssikkerhet på reise med forhøyet etterretningstrussel

Fremmede sikkerhets- og etterretnings-tjenester har større handlingsrom til å innhente informasjon om deg i utlandet. I land som utgjør en særlig etterretningstrussel mot Norge og i land hvor disse har stor tilstedeværelse, samt i totalitære stater, så vil sikkerhets- og etterretningstjenester ofte ha en lav terskel og betydelig kapasitet til å gjennomføre målrettet etterretningsvirksomhet. Virksomheten kan både rettes mot deg og mot personer som du er i kontakt med. De kan benytte virkemidler som for eksempel hemmelig ransaking, avlytting, overvåking av trådløst nettverk, innhenting av teletrafikk og fysisk kontroll av deg og din bagasje. Som myndighetsperson må du forutsette at besøket ditt er forhåndskjent for sikkerhets- og etterretningstjenestene, både i transittlandene og på destinasjonen for reisen.

Ved reiser til utsatte land bør du gjøre en grundig vurdering av i hvilken grad og på hvilken måte skjermingsverdig informasjon skal medbringes og eventuelt hvordan den skal oppbevares. Sett deg godt inn i lovverk, instruks og din egen organisasjons/ virksomhets retningslinjer for behandling av skjermingsverdig informasjon, samt bruk av IKT-utstyr på reiser til utlandet.

Råd for informasjonssikkerhet før reisen

- Ved reiser til steder med høy risiko så anbefales det å ta med utstyr som utelukkende skal benyttes på reisen. Aldri logg inn på dine egne kontoer på låneutstyr, skadevare kan smitte via skyer og infisere ditt private utstyr.
- Ta med minst mulig sensitiv eller skjermingsverdig informasjon på reisen.

Råd for informasjonssikkerhet under reisen

- Unngå bruk av trådløst nett og blåtann.
- Bruk aldri offentlige eller åpne trådløse nett. Bruk i stedet mobildata eller mobilt bredbånd.
- Ikke last ned ny programvare eller oppdateringer under reisen med mindre de er viktige sikkerhetsoppdateringer.
- Ikke legg igjen digitalt utstyr eller sensitiv informasjon som for eksempel på hotellrommet. Forutsett at ansatte på hotellet har tilgang til både rommet ditt og safen.
- Benytt forseglingspose uten innsyn til skjermen hvis du likevel må legge fra deg ditt digitale utstyr.

Råd for informasjonssikkerhet etter hjemkomst

- Hvis du har benyttet utstyr kun beregnet på reisen så hold dette strengt adskilt fra ditt eget og organisasjonens.
- Fortsett å være kritisk til uventede og ukjente sikkerhetsvarsler, e-poster, vedlegg og bilder som du eventuelt får tilsendt.
- Hvis du tror at du kan ha vært utsatt for tilnærminger eller andre former for kontakt fra utenlandske etterretnings- og sikkerhetstjenester så er det svært viktig at du rapporterer dette til PST og til sikkerhetsorganisasjonen i din egen virksomhet/organisasjon uten opphold. Oppmerksomhet fra fremmede aktører kan også inntreffe etter at du har kommet hjem fra reisen.

Varsling

- Hvis du opplever at det er fare for liv og helse så utløs eventuell alarm eller ring politiets nødnummer **112**.
- Ved andre straffbare forhold eller bekymringer, ring **02800**, som går til politiet der du befinner deg.
- Trusler mot myndighetspersoner (som ikke er akutte) varsles i etablerte kanaler eller til PSTs døgnåpne responscenter: **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 kan være relevant for både PST og politiet. Dette kan danne grunnlag for både konkrete sikkerhetsvurderinger og tiltak, og opprettelse av straffesaker.

Kilder

Håndboken er skrevet og publisert av Politiets sikkerhetstjeneste. Enkelte av rådene bygger på innspill fra andre relevante sikkerhetsmyndigheter.

Les mer:

- På nsm.no kan du finne utfyllende råd om blant annet digital sikkerhet på reiser.
- På Utenriksdepartementets (UD) hjemmesider regjeringen.no finner du reiseinformasjon om innreise, naturforhold og andre relevante opplysninger for nærmere 200 land. Utenriksdepartementet gir også reiseråd når de mener at norske borgere ikke bør dra til et land eller et område.
- [Reiseregistrering.no](https://reiseregistrering.no) er et tilbud om å registrere dine kontaktopplysninger hos UD. Dersom det skjer en alvorlig hendelse så har UD dermed mulighet til å sende deg informasjon og tilby hjelp.
- Kommunal- og distriksdepartementet har med faglig bidrag fra Politidirektoratet og Politiets sikkerhetstjeneste laget publikasjonen «Veileder om forebygging og håndtering av hatefulle ytringer, hets og trusler mot politikere og kandidater» som finnes på nettsiden hatogtrusler.no
- Kommunal- og distriksdepartementet har også med faglig bidrag fra Etterretningstjenesten, NSM og PST laget veilederen «Gode sikkerhetsråd til deg som stiller til valg» som også finnes på regjeringen.no
- På nettsidene til Politiets sikkerhetstjeneste [PST.no](https://pst.no) kan du blant annet lese mer om Nasjonale trusselvurderinger, høre podkaster om aktuelle tema, lese mer om råd mot terrorhandlinger og finne denne veilederen i elektronisk utgave.
- På [Politiet.no](https://politiet.no) kan du anmelde enkelte forhold og finne informasjon om blant annet hat, ytringer og trusler.

Vurdering av bekymringsfulle hendelser

Skjemaet gir en veiledning i å identifisere hendelser, henvendelser eller ytringer fra personer eller aktører som bør 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 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 guddommelig oppdrag o.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.		

(1-7 = varsle PST eller politiet)

(8-14 = varsle internt. Vurder å varsle PST eller politiet særlig ved flere forhold.)

