Personlig säkerhet

Säkerhetspolisen


Kommunstyrelsens
sammanträdesrum

För dig som är politiskt aktiv

Genom riskanalyser, aktiva val och medvetna förhållningssätt kan du som är politiskt aktiv värna om din personliga säkerhet.

I handboken Personlig säkerhet ges exempel på förebyggande åtgärder och skyddsåtgärder som kan användas för att förhindra eller avstyra hotfulla situationer om de skulle uppstå. Här behandlas allt från hur du kan tänka kring sociala medier till hur du ska agera vid ett eventuellt terrorattentat.

Boken är primärt skriven för politiskt aktiva, men råden fungerar lika väl för andra utsatta yrkesgrupper.

Boken kan med fördel användas som diskussionsunderlag då ni tillsammans utformar ert säkerhetsarbete.

Produktion: Säkerhetspolisen. Andra upplagan 2018. **Grafisk form:** Yours. **Foto:** Ulf Huett och Micke Lundström. **Typografi:** Eurostile och Swift. **Papper inlaga:** 130g Amber graphic. **Papper omslag:** 300g Amber Graphic. **Tryck:** Stibo Graphic. **ISBN:** 978-91-86661-13-7.

Innehåll

Förord av Säkerhetspolischefen 06-07

Säkerhet vid politiskt arbete **08-11**
Skydd av person 10-11

Riskanalys och medvetna val i vardagen **12-21**
Arbetsplatsen 14-15
Exponering i massmedia 16-17
Sociala medier 18-19
Kontroverser och ryktesspridning 20-21

Kampanjarbete och offentliga möten **22-25**
Säkerhet vid offentliga möten, Dörrknackning 23-24
Säkerhet vid bilfärder 25

Hantera hot och angrepp **26-34**
Hot på telefon, Hot via internet 28
Hantering av hotbrev, Avvikande försändelser 29
Stalkning - att bli förföljd 30-31
Rättshaverister, Utpressning 32-34

Skydda din identitet och integritet **35-43**
Mobiltelefoner och trådlösa nätverk 36-37
Offentliga datorer och nätverk, ID-kapning 38-41
Påverkansoperationer, Personliga möten i syfte att värva 42-43

Säkerhetsåtgärder i bostaden och vardagen **44-53**
Dörrar, brevinkast, fönster och glasade ytor, nycklar, kort och koder 45-47
Familj - skyddet för närstående 48-49
Larm och skyddsåtgärder 50-51
Larma med mobilen 52-53

Anmäl alla hot! **54-57**
Kontaktförbud 56-57

Resor - inrikes och utrikes **58-61**
Konfliktdrabbade områden 60
Transfer från flygplatsen, Taxiresor, Säkerhet på hotellet 61

Allvarliga händelser utomlands **62-63**

Terrorangrepp och andra attentat **64-65**

Förord

En tydligare polarisering i vårt samhälle, ett hårdare debattklimat och en ökad exponering av den enskilda personen. Till det kan tilläggas att hotbilden mot Sverige och svenska intressen har förändrats. Som politiker och offentlig person behöver du i dag tänka på säkerhet ur flera perspektiv.

Säkerhetspolisen har tillsammans med Polismyndigheten i uppgift att skydda Sveriges demokratiska system, medborgarnas fri- och rättigheter och den nationella säkerheten. Tillsammans ska vi motverka hot, våld och trakasserier som påverkar det demokratiska systemet. I det arbetet ingår att motverka de krafter som med otillåtna medel försöker påverka den fria debatten, det politiska beslutsfattandet och verkställandet av politiska beslut. Det är bakgrunden till att Säkerhetspolisen nu ger ut en uppdaterad version av boken Personlig säkerhet. Boken ger dig råd kring din personliga säkerhet. Den utgåva som du nu håller i din hand har anpassats efter dagens samhällsklimat och förutsättningar.

Som offentlig person kan du ha ansvar över eller inflytande i en viss fråga. Om den blir särskilt uppmärksammad eller väcker debatt finns en risk att du utsätts för hot eller trakasserier. Det ska ses i ljuset av ett hårdare debattklimat och att många av oss i större utsträckning än tidigare exponeras i sociala medier. Samtidigt sker en ökad polarisering i de grupper i samhället som uppmanar andra eller själva kan tänka sig att använda hot, våld eller trakasserier för att uppnå sina mål.

Risken att bli utsatt ser givetvis olika ut från person till person, från uppdrag till uppdrag och från tid till annan. Gemensamt är dock att det är ett hot mot vår demokrati om du som är politiker inte vågar fatta beslut på grund av upplevt obehag eller faktiska hot och trakasserier. På senare år har flera åtgärder vidtagits för att öka tryggheten för våra politiker – och även för andra yrkesgrupper som är utsatta för hot.

Sommaren 2017 beslutade regeringen om en handlingsplan för att förebygga

Det är ett hot mot vår demokrati om du som är politiker inte kan fatta beslut på grund av upplevt obehag eller faktiska hot och trakasserier.

och hantera hot och hat mot bland andra politiker och journalister. Vidare har Sveriges kommuner och landsting (SKL) genomfört ett arbete för att stödja kommuner, regioner och landsting i deras förebyggande arbete mot hot och våld mot förtroendevalda. Samtidigt arbetar Polismyndigheten med stöd och information för säkerhetsansvariga och politiska partier på kommunal nivå.

Parallellt med detta har vi inom Säkerhetspolisen vårt grundläggande uppdrag att skydda Sverige och vår demokrati. Våra politiker i regering och riksdag ska ha möjlighet att utföra sina uppdrag utan att utsättas för hot eller våld. Vi ska också arbeta för att minska risken för påverkansoperationer och elektroniska angrepp genom ett ökat säkerhetsskydd.

I den här handboken är din säkerhet i fokus och råden ska ses som ett stöd i ditt arbete. Säkerhet måste balanseras mot ett öppet samhälle och vårt mål är att öka säkerhetsmedvetandet och tryggheten för såväl dig som är politiker inom den centrala statsledningen som för dig som arbetar i våra kommuner, landsting och regioner. På så sätt bidrar vi till att säkra det demokratiska systemet.

Handboken är framtagen i nära samverkan med Polismyndigheten. Ett nära samarbete har också skett med säkerhetsansvariga vid Riksdagsförvaltningen. Dessutom har Regeringskansliet, Sveriges kommuner och landsting (SKL), Myndigheten för samhällsskydd och beredskap (MSB), Brottsförebyggande rådet (Brå) samt ett flertal andra berörda myndigheter och experter bidragit i arbetet med boken.

Anders Thornberg,
säkerhetspolischef

I Brås rapport Politikernas trygghetsundersökning från 2017 framgår att 25 % av Sveriges förtroendevalda utsatts för hot, våld eller trakasserier under 2016. Två grupper är särskilt utsatta:

- Yngre förtroendevalda (upp till 29 år) där nästan 40 % uppger att de blivit utsatta.
- Kvinnliga förtroendevalda i ordförandeposition där 41 % anger att de blivit utsatta.

Bland de förtroendevalda som blivit utsatta uppger sedan 44 % att deras politiska uppdrag har påverkats till följd av detta. Nästan en tredjedel (29 %) uppger att de som en följd av utsattheten självcensurerat sig.

Säkerhet vid politiskt arbete

Som politiskt aktiv har du det demokratiska uppdraget att diskutera och föra ut de frågor som dina väljare och ditt parti står för. För att du ska kunna göra detta finns det flera faktorer som spelar in. En viktig faktor är att du ska känna dig trygg och säker. Detta gäller oavsett politiskt parti eller var på den politiska arenan du är verksam.

Det är väsentligt att både du som enskild politiker och att ni tillsammans som organisation regelbundet lyfter säkerhetsfrågor och utbildar er i ämnet. Dessutom finns experter att ta hjälp av för att skapa trygga förhållanden. Säkerhet byggs tillsammans med andra i ett kontinuerligt utbyte och återkommande dialog.

Det finns krafter som vill begränsa den demokratiska processen. Detta har flera orsaker, men konsekvensen av de krafternas agerande kan vara att du inte utövar dina demokratiska rättigheter fullt ut. Det sker relativt få brott i den politiska vardagen. Men du som politiker kan ändå utsättas för obehagliga situationer som i sig kanske inte är olagliga men som gör att du begränsar dig eller undviker att engagera dig i en viss fråga. Det finns också individer, grupper och organisationer som är beredda att använda brott - som hot, våld eller trakasserier - för att påverka och till och med hindra dig från att fatta vissa beslut eller ta ställning i vissa frågor.

Naturligtvis ska du föra ut dina frågor i de kanaler och forum som finns. Men en bieffekt av att exponeras i exempelvis massmedia kan vara att risken för hot, trakasserier eller angrepp ökar. Den ökade risken kan bland annat bero på att någon håller dig personligt ansvarig för ett politiskt beslut eller för utvecklingen inom ett visst område.

Det händer också att individer blir besatta av en offentligt exponerad person på andra grunder än de politiska ställningstaganden du representerar. Det kan exempelvis röra sig om en inbillad romans. Du kan dessutom mer slumpmässigt hamna i fokus för en så kallad rättshaverist.

Om du är engagerad i en fråga som direkt eller indirekt gäller rikets säkerhet kan du även bli föremål för spionage eller bli utsatt för en så kallad påverkansoperation.

Skydd av person

Beroende på var du utövar din politiska gärning handhas skyddet av din personliga säkerhet av olika aktörer. Om du är fritids-, kommun- eller landstingspolitiker är det den regionala polisens brottsoffer- och personsäkerhetsgrupp som ansvarar för hotbildsbedömning och skyddsåtgärder om du blivit utsatt för ett brott. För den centrala statsledningen, där riksdag och regering ingår, är det Säkerhetspolisen som ansvarar för hotbildsbedömningar och skyddsåtgärder. De flesta bevakningsbolag har också personskyddstjänster och teknisk utrustning för person- och egendomsskydd.

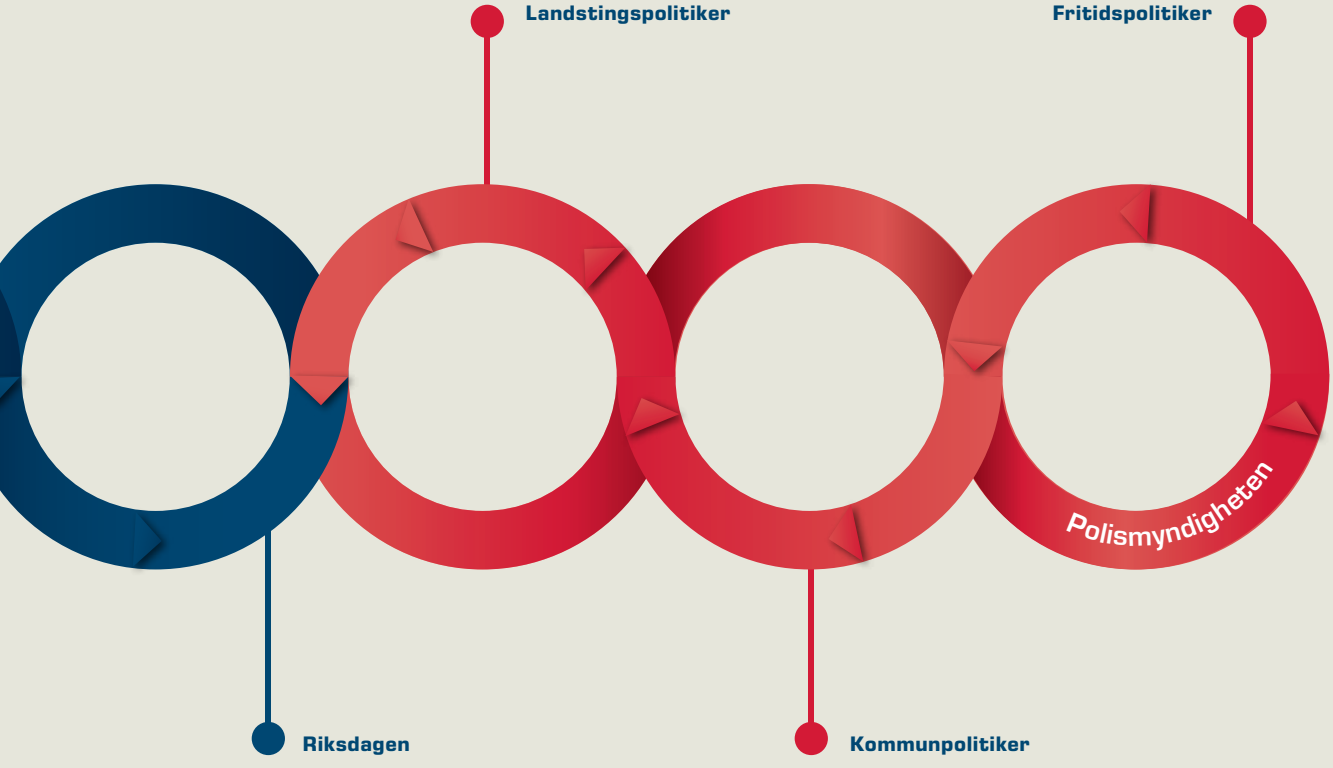
Oavsett vem som tar hand om skyddsåtgärderna så utformas de utifrån hur just din situation ser ut. En noggrann bedömning av risken för hot och angrepp görs. Det kan till exempel röra sig om olika tekniska skyddsåtgärder, som att installera lås och larm eller använda sig av personbevakning.

Polisens personsäkerhetsarbete

Polisens personsäkerhetsarbete erbjuder hotade personer och deras anhöriga skydd, hjälp och stöd. Personsäkerhetsarbetet vänder sig till alla människor som är i behov av polisiära skyddsinsatser. Exempel på personer som kan komma ifråga vid personsäkerhetsarbete är kommunpolitiker, personer som är utsatta för hedersrelaterat våld, hotade kvinnor, journalister, egna företagare, restaurangägare, poliser och åklagare.

Det är den lokala brottsoffer- och personsäkerhetsverksamheten (Bops) som i första hand ska ägna sig åt det grundläggande personsäkerhetsarbetet. Detta görs i samverkan med olika berörda myndigheter, till exempel Säkerhetspolisen, kommunen och Skatteverket.

Mydigheternas ansvarsfördelning



Det är antingen Säkerhetspolisen eller Polismyndigheten som ansvarar för skyddsarbetet på den politiska arenan. Ovan ser du vilken myndighet som ansvarar för vilka funktioner. De blå ringarna är Säkerhetspolisens ansvar och den samlade termen för dessa är den centrala statsledningen. Till den centrala statsledningen räknas även talmannen, statssekreterarna, kabinettssekreteraren och tronföljaren. I de röda ringarna ligger ansvaret hos Polismyndigheten.

Riskanalys och medvetna val i vardagen

Du har precis lämnat en trevlig tillställning inne i centrum och klivit ut i mörkret på gatan. Det är kallt, men du känner för att ta en kort promenad hem efter att ha suttit still i flera timmar. Du hör att det är ganska stökigt i kvarteret men du vet att gatorna bortom dessa är lugnare.
Ska du välja att promenera hem?

Ovanstående situation är ett exempel på en riskanalys. Vi gör alla sådana analyser i vår vardag. En riskanalys är den process där du, medvetet eller omedvetet, identifierar risker och bedömer åtgärder du kan vidta för att undvika eller minimera dessa risker.

En riskanalys kan också vara mer detaljerad än exemplet ovan och då omfatta särskilda aktiviteter eller säkerhetsåtgärder för en specifik situation. Ett exempel är de säkerhetsåtgärder du gör inför en lång resa, med allt från att du larmar hemmet, ger dina anhöriga adresser och resplaner, till var du placerar ditt pass och dina resehandlingar. En riskanalys kan också göras särskilt för personer som är utsatta för hot.

I och med ditt politiska engagemang bör du och dina närmaste kolleger regelbundet reflektera och analysera om ni är utsatta för risker. Försök att bedöma eventuella konsekvenser och reaktioner på saker ni gör eller har gjort, till exempel beslut som ska fattas eller uttalanden som ska göras. Ha gärna det som utgångspunkt när du läser den här boken.

Genom att förbereda dig, medvetet kunskapshöja dig, samverka och göra aktiva val är du med och bygger din säkerhet.

Steg i en riskanalys

Vilka aktiviteter behöver du analysera särskilt? Är det ett framträdande, ett känsligt beslut eller ett uttalande i en fråga som kan uppfattas som negativt eller kontroversiellt?

Finns det information du behöver samla in eller en sakkunnig du bör rådgöra med?

Vilka åtgärder kan du vidta för att minska risken?

Var och när är det störst risk för att du bli utsatt för ett påhopp eller angrepp? Vilka möjligheter till skydd finns vid en hotfull situation? Vilka möjligheter finns att larma och snabbt få hjälp om något skulle hända?

Tänk också på att hotfulla situationer kan ha sin upprinnelse i händelser som ligger långt tillbaka i tiden.

Arbetsplatsen

De flesta av oss reflekterar inte så mycket över de entréer vi passerar eller de lås, koder och inpasseringskort som vi använder för att nå fram till vår arbetsplats. Men som en förberedande åtgärd är det klokt att ta reda på vad som gäller kring säkerheten på din arbetsplats eller i er partilokal.

Generellt kan det sägas att offentliga byggnader och myndigheter ska vara öppna för medborgare och besökare, men ofta finns olika typer av säkerhetshöjande åtgärder och ett visst tillträdesskydd brukar gälla. Informera dig om aktuella skyddsåtgärder genom att fråga säkerhetsansvariga eller din närmaste chef.

Se till att det finns en rutin kring hur ni hanterar oanmälda besökare. Informera berörda medarbetare om exempelvis offentliga möten där frågor som kan uppfattas som kontroversiella ska debatteras och många deltagare förväntas delta så att ni tillsammans har en tanke kring hur ni ska bemöta obehagliga situationer.

Undvik att ta emot okända besökare i enrum. Är du osäker på situationen eller misstänker att något obehagligt kan uppstå, be någon att sitta med på mötet. Förbered dig också så att du enkelt kan lämna rummet och larma om du blir hotad eller angripen. Det är klokt att alltid eskortera besökarna i lokalerna och inte lämna obehöriga utan uppsikt. Var uppmärksam på kvarglömda väskor och annat som kan innehålla farliga föremål.

Ytterligare ett råd är att variera färdväg och restider om det finns risk för att du kan utsättas för angrepp.

Ta reda på vilka säkerhetsrutiner som gäller. Tala med säkerhetsansvariga eller din parti-organisation.

Exponering i massmedia

Som politiskt aktiv är det både vanligt och eftersträvansvärt att exponeras i media. Men fundera alltid i förväg på hur och var du vill visa upp dig.

Om någon vill intervjua dig bör du undvika ditt hem och föreslå att ni ses på en neutral plats. Exempelvis någonstans som har med din fritid att göra men där du trots det inte vistas återkommande. Om du till exempel är naturintresserad kan du och reportern ses utomhus. Om du är sport- eller kulturintresserad stäm träff i en sådan miljö. Du bör generellt undvika att exponera ditt hem, din familj och de exakta miljöer där du regelbundet befinner dig.

Du bör aldrig uttala dig om eller kommentera din egen säkerhet eller olika skyddsåtgärder som rör dig eller din familj. Detta är särskilt viktigt att tänka på vid mediekontakter då dina uttalanden kan få stor spridning och sedan hamna hos en eventuell gärningsperson.

En annan viktig sak att minnas är att aldrig kommentera till media eller uppdatera i sociala medier i affekt, exempelvis då något obehagligt precis har skett så som vid en olycka eller om du precis blivit hotad.

Du bör också tänka på att även om du inte själv är utsatt kan en arbets- eller partikamrat vara det. Undvik därför att nämna dem i intervjuer eller i kontakter med media utan att det är förankrat hos dem. På samma vis ska du undvika att exponera dem i sociala medier. Om du har några pressansvariga på din arbetsplats eller i ditt parti, rådgör med dem om du känner dig osäker. Ni kan till exempel förbereda er tillsammans och ha en policy för kriskommunikation.

Om du blir utsatt för hot ska du alltid polisanmäla detta.

Du bör aldrig uttala dig om eller kommentera din egen säkerhet eller olika skyddsåtgärder som rör dig eller din familj.

Sociala medier

Inte ens en politiker är skyldig att fortsätta svara i digitala kanaler när debatten och språkbruket hamnat bortom rimliga gränser.

Sociala medier är en viktig arena för politiker. Den bevakas även av massmedia och det finns ett stort intresse för politikers digitala närvaro.

Sociala medier är ett enkelt sätt att nå dina väljare och kompletterar de övriga kommunikationskanalerna. En av fördelarna med sociala medier är att det är en plats där flera olika målgrupper samlas. Men detta ställer också krav på en medvetenhet om hur du agerar och uttrycker dig. Det är en god idé att tydligt definiera vad du och dina kolleger vill uppnå med ert användande av sociala medier. Reflektera även över val av språkbruk och hur det stämmer överens med din personlighet och det uppdrag du fått. Det kan vara en fördel att du, tillsammans med dina medarbetare, väljer ut några kanaler och tillsammans motiverar varför kanalerna ska användas och vad de ska fyllas med. Formulera gärna en gemensam policy.

Debatter är en viktig del av det demokratiska samtalet. I digitala kanaler kan det dock finnas situationer där du möter individer vars enda syfte är att smutskasta eller förstöra samtalet. Vid sådana tillfällen är det viktigt att inte dras in i deras språkbruk. Tänk istället på att merparten av nätanvändarna är tysta betraktare varav de flesta förväntar sig att du ska agera klokt.

Kom också ihåg att inte ens en politiker är skyldig att fortsätta svara i digitala kanaler när debatten och språkbruket hamnat bortom rimliga gränser. Jämför med samma situation på ett evenemang. Hur hade du hanterat den då? Använd blockeringsfunktioner på tjänster vid behov.

Allt tyder på att den digitala arenan kommer fortsätta att vara viktig för politiken. Därför är det också viktigt att ha en genomtänkt strategi.

Vägledning i sociala medier

Undvik att i förväg, eller under ett pågående möte, berätta var du befinner dig. Använd inte incheckningsfunktioner som avslöjar din geografiska position.

Berätta om saker du har gjort - och inte om vad du ska göra. Detta för att undvika kartläggning eller att personer söker upp dig.

Undvik att exponera eller ge en inblick i dina vanor som kan underlätta kartläggning av dig, såsom tränings- eller shoppingrutiner eller platser du regelbundet besöker.

Var personlig men inte privat i dina inlägg. Definiera vad personligt betyder för dig och vilka dina gränser är. Skapa en genomtänkt hållning för hur, vad och när du kommunicerar i sociala medier utifrån din egen säkerhet.

Var noga med att alltid fråga om godkännande för publicering från de personer som medverkar i dina inlägg och på dina bilder.

Var noga med att även i privata sammanhang berätta vad som gäller för din medverkan i sociala medier. Be även vänner och familj att undvika angivelse av geografisk plats om du medverkar på bild. Detta även för tjänster du inte själv använder.

Betrakta så kallade ”direktmeddelanden” på sociala medier som offentliga arenor. Allt som sägs där ska teoretiskt sett hålla för att granskas av såväl massmedia som av meningsmotståndare.

Vid direkt hot ska du skärmdumpa inläggen och användarprofilen samt vända dig till säkerhetsansvariga och polis. Här gäller nolltolerans och rutinerna bör finnas formulerade i policyn.

Kontroverser och ryktesspridning

Sociala medier gynnar material som manar till engagemang och reaktioner. Samtidigt sprids information fortare och till fler än någonsin förut. Utvecklingen av den moderna informationsmiljön - i form av sociala medier, digitala plattformar och andra tjänster - används i alla sammanhang. Sammantaget innebär det att plötsliga och ibland storskaliga kontroverser kan uppstå.

Det vill säga att det som publicerats snabbt får spridning, oavsett om informationen är sann, falsk, vilseledande eller populistisk. Spridningen kan i sin tur leda till starka reaktioner och än starkare motreaktioner oavsett om informationen publicerats av dig, eller någon annan.

Det som publicerats behöver inte vara tänkt att väcka starka reaktioner. Det kan hända oavsett intention och formulering. Risken för att bli föremål för storskaliga och plötsliga kontroverser är särskilt hög om man är en offentlig person, som politiker, journalist eller opinionsbildare. Det vill säga funktioner som driver frågor där många har starka åsikter.

Det innebär att du som politiskt aktiv och den organisation du arbetar i behöver ha en utformad plan för hur ni ska agera. Hotbilden kan höjas på kort tid och det kan uppstå behov av att snabbt efterforska, nyansera eller dementera uppgifter som cirkulerar. En utarbetad plan hjälper er också att vidta eventuella säkerhetsåtgärder om situationen skulle bli mycket allvarlig.

Har din partiorganisation rutiner för hur ni hanterar snabb ryktesspridning i sociala medier?


Kungsgatan

Kampanjarbete och offentliga möten

Under en valrörelse är engagemanget och tempot högre än vanligt. Då kan det vara lätt att tappa fokus på din egen säkerhet. För att underlätta säkerhetsarbetet bör du och dina kolleger ha rutiner kring exempelvis hur många ni ska vara i en valstuga eller då ni knackar dörr. Ni bör också ha rutiner för att stämma av säkerheten varje dag. Håll er också uppdaterade om de senaste rönen via utbildningar och seminarier.

Säkerhet vid offentliga möten

När du själv eller ditt parti arrangerar ett offentligt möte bör ni rådgöra med säkerhetsansvariga om de rutiner som finns.

Gör en riskanalys

Bedöm även om det är något som påverkar hur mötet bör genomföras. Kan personen/ämnet/platsen/lokalen påverka säkerheten? Är det en kontroversiell fråga som ska diskuteras eller är platsen särskilt utsatt? Om du och dina kolleger vet att de frågor som ska lyftas under mötet varit hårt kritiserade bör ni beakta detta och ha en plan för hur ni eller andra med ansvar för säkerheten ska agera om stämningen blir obehaglig.

Bedöm behovet av resurser och bevakningsåtgärder som krävs för säkerheten. Samverka med Polismyndigheten eller Säkerhetspolisen, beroende på vilken politisk arena du verkar på. Informera er om tillståndsfrågan via Polismyndigheten.

I dialogen med polisen bör ni också informera dem om eventuellt kontroversiella budskap. Ta också reda på om de känner till andra evenemang, om till exempel en demonstration ska hållas parallellt med ert möte.

Bedöm också i god tid vilken information ni ska gå ut med inför mötet. Exempelvis vilka uppgifter kring mötet som ni kommunicerar i sociala medier. Var noggrann med vilka som informeras om detaljerna i programmet. Ni bör även undvika att uppgifter som när ni anländer till hotell, när ni ska äta middag och liknande kommer ut till obehöriga.

Placering av scen och talarpodium

Målsättningen bör vara att huvudpersonen ska ha ”ryggen fri” med skyddad bakgrund eller fond. Undvik därför platser mitt på en yta med folk runt omkring. Tänk på angreppsrisken från personer och det eventuella kastavståndet till scen.

Planera för avspärrning

Säkerhetsavståndet till talaren kan markeras genom exempelvis rep, band eller blommor. Tänk på placering av entréer och av vakter eller funktionärer utifrån säkerhetssynpunkt. Tänk även på var ni placerar eventuella journalister.

Förbered kommunikation

Upprätta bra kommunikationsvägar med bevakningen. Lägg in kortnummer i din mobil till alla viktiga kontakter som polis och väktare. Vid akut läge ring nödnummer 112. →

Ha beredskap för störningar

Förbered för att tidigt kunna hantera incidenter och spontana störningar som kan uppstå under evenemanget. Tänk på att inte provocera störande eller hotfulla personer. Förbered åtgärder och rollfördelning på plats för en eventuellt hotfull situation.

Planera vägen ut

Förbered en reträttväg till ett säkert utrymme ifall en hotfull situation skulle uppstå.

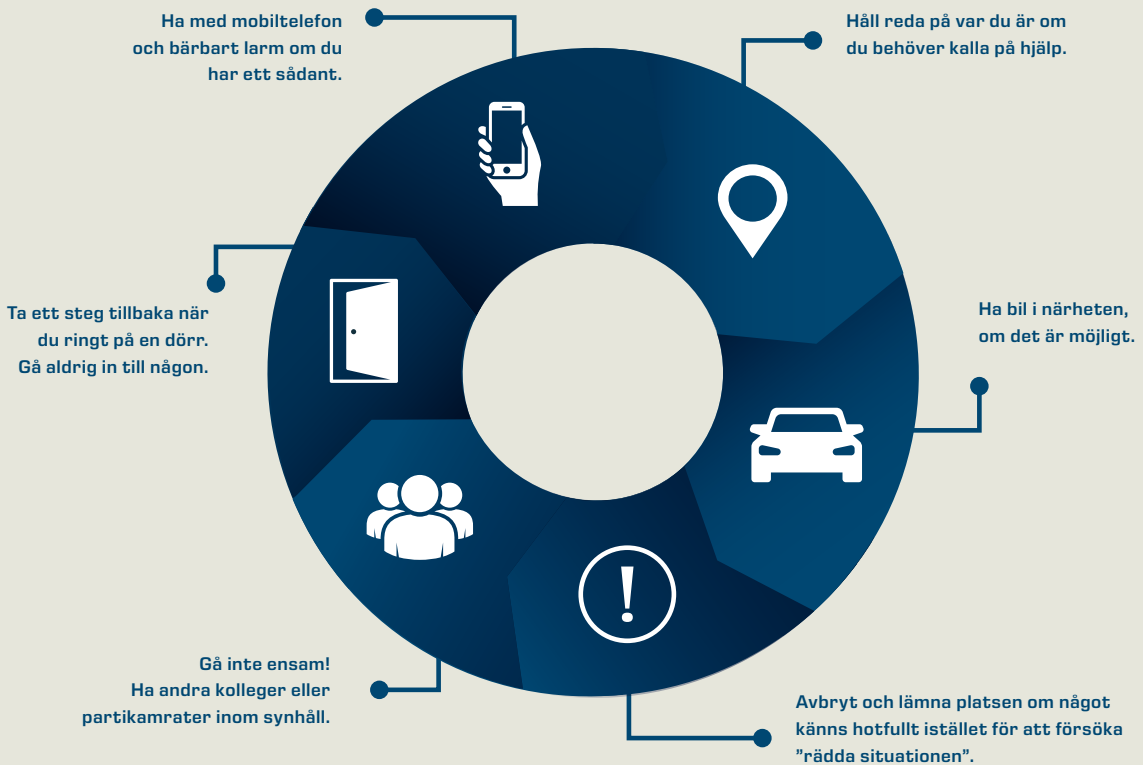
Ha även en säker parkeringsplats i nära anslutning till scenen. Undvik också att släppa in eller tillåta okända fordon att parkera i närområdet. Rör er alltid tillsammans till och från evenemanget.

Säkerhet vid dörrknackning

Som politiskt aktiv kan du komma att delta i olika slags kampanjer. Vid kampanjer genom dörrknackning finns det flera delar att beakta.

Se figuren nedan.

Säkerhet vid dörrknackning



Säkerhet vid bilfärder

Din bil kan vara en säker plats för att skydda sig i eller en plats för att hastigt lämna ett farligt område, men den kan också vara en plats där du är extra utsatt.

Om du hamnar i en situation där du känner dig hotad bör du undvika att stiga ur bilen och ta direktkontakt. Du kan undvika det genom att kommunicera genom bilrutan, kalla på hjälp eller ta dig till en plats där det finns andra människor. Ha för vana att alltid ha låsta dörrar under bilfärden.

Om du misstänker att du är utsatt för någon typ av kartläggning är det bra att variera färdväg och restider. Ett råd som ges vid förhöjd hotbild är att använda sig av säkra parkeringsplatser, exempelvis ett väl skyddat garage utan koppling till din bostadsadress.

Billarm som är kopplat till bilens låsfunktion används för att motverka skadegörelse och stöld samt för att se om någon har öppnat eller rört bilen. Förvissa dig alltid om att det fjärrstyrda centrallåset fungerar och att dörrarna verkligen går i lås. Det finns även speciella larm – så kallade paniklarm – som gör att du kan larma för att få hjälp. De fungerar så att du med hjälp av nyckeln eller en fjärrkontroll kan utlösa ett larm i form av en ljus- eller ljudsignal för att väcka uppmärksamhet. En del bilmodeller har denna funktion som standardutrustning.

Om du använder taxi ska du helst förbeställa bilen och endast spontanåka med taxiregistrerade bilar och med chaufförer som har taxilegitimationen väl synlig.

Ha för vana att alltid låsa bildörrarna under färden.

Hantera hot och angrepp

Om du skulle bli utsatt för hot, våld eller trakasserier är det bra att känna till hur dessa situationer ska hanteras. Detta oavsett om situationen skulle uppstå i samband med ett offentligt framträdande, på nätet, på arbetsplatsen eller i anslutning till din bostad.

Om du blir utsatt för hot som kan knytas till din politiska gärning eller ditt uppdrag bör du vara extra uppmärksam på vad som sker. Att vara mentalt förberedd kan hjälpa dig att agera korrekt. Det kan handla om att du i förväg har tänkt på olika scenarier och har sett olika handlingsalternativ framför dig.

Din direkta reaktion blir kanske att snabbt radera ett hotfullt meddelande. Men för att någon ska kunna lagföras är det viktigt att du spelar in eventuella hotfulla samtal och sparar de meddelanden du får. Om du blir hotad ska du självklart kontakta polisen som kan ge dig råd i hur du ska agera. Du ska också informera din interna säkerhetsansvarige.

En hotfull situation kan handla om bland annat påträngande personer, oönskade påhälsningar och gåvor. Hot kan också framföras via exempelvis brev, telefon, e-post eller på sociala medier. Ett första råd är att försöka hålla sig lugn. Om du är uppmärksam på vad som händer kan du anpassa ditt sätt att agera utifrån situationen och hur denna förändras. Försök att vara saklig även om du utsätts för provokationer.

Om du samtalar med en person kan du försöka få denne att bryta sitt handlingsmönster genom att föreslå alternativ till dennes agerande. Om du känner dig hotad bör du försöka bedöma vilken avsikt personen har och sedan avgöra hur du ska agera. Det kan handla om att du måste ropa på hjälp, fly från platsen eller försvara dig.

Handla alltid med eftertänksamhet. Lita på dig själv och din förmåga att hitta en utväg. Försök agera med initiativ och handlingskraft. Lita på din intuition om du hamnar i en situation där du får en obehaglig känsla kring en person.

Nödvärn

Var och en har rätt att försvara sig själv och sin egendom, och har då rätt att använda det våld som inte är uppenbart oförsvarligt. En person som hjälper den som angrips har samma rätt. Rätten till nödvärn gäller mot:

- *Påbörjat eller överhängande brottsligt angrepp på person eller egendom.*
- *Den som med våld eller hot om våld eller på annat sätt hindrar att egendom återtas på bar gärning.*
- *Den som olovligen trängt in i eller försöker tränga in i rum, hus, gård eller fartyg, eller den som vägrar att lämna en bostad efter tillsägelse.*

Hot på telefon

Om du blir hotad eller trakasserad via telefon bör du snarast anmäla det till polisen. I en eventuell brottsutredning finns det möjlighet att spåra samtal – både sådana som har gjorts och att skapa en beredskap för att spåra eventuella framtida samtal. Spårning av samtal kan ske för både fast och mobil telefoni. Det finns vissa tekniska begränsningar, där en försvårande faktor kan vara oregistrerade kontantkort. Men i vissa fall är det möjligt att spåra även dessa.

Du kan själv begära ut listor på inkommande samtal från din teleoperatör. Tjänsten finns hos de flesta teleoperatörer, men förutsättningarna för samtalsspårning skiljer sig mellan olika bolag. Du bör därför tillsammans med din säkerhetsansvarige eller motsvarande kontakta din teleoperatör för information om tjänsten och dess förutsättningar.

Lyssna uppmärksamt och avbryt inte den som ringer. Notera tid, bakgrundsljud, kön, ålder, dialekt och liknande. Upprepa det som den uppringande säger och låtsas som att du inte hör ordentligt. Använd fraser som ”Förlåt, jag hörde inte riktigt vad du sa?” På så sätt förlängs samtalet vilket kan ge dig mer information och därmed underlätta identifieringen av den uppringande.

Hot via internet

Hot och trakasserier via internet ökar. Har du utsatts eller misstänker att du kan utsättas kan du i vissa fall få hjälp av din internetleverantör genom att åberopa så kallade netikettsregler, som är operatörens regler för uppförande på nätet. I allvarliga fall eller om du utsätts för direkta hot bör du ta kontakt med polisen. Tänk på att inte radera de hot du får via internet, polisen behöver dem i digital form för att kunna spåra vilken dator de har skickats från.

Gör skärmdumpar på det du kan. Vid behov kan polisen hänvisa ärendet vidare till sina specialister på it-relaterad brottslighet.

24 kap. 1 § brottsbalken

Olaga hot enligt 4 kap 5 § brottsbalken: Om någon lyfter vapen mot annan eller eljest hotar med brottslig gärning på sätt som är ägnat att hos den hotade framkalla allvarlig fruktan för egen eller annans säkerhet till person eller egendom, döms för olaga hot.

Avvikande försändelser

Post som du får hem eller till din arbetsplats kan innehålla obehagliga överraskningar. Du bör därför vara uppmärksam på obeställda och avvikande försändelser och du bör be din familj agera på samma sätt.

Hantering av presenter

Paket bör helst avemballeras av givaren själv. Vid misstänkt försändelse; rör eller öppna inte, larma polisen.

Kontakta polisen om du får ett paket som ser annorlunda ut och där du inte känner igen avsändaren. Försök inte öppna det för att se efter vad det är.

Var uppmärksam på försändelser som har:

- Ojämnt eller buckligt utseende.
- Avvikande vikt, det vill säga ovanligt lätt eller tungt i förhållande till storleken.
- Fettfläckar på kuvertet eller omslaget eftersom sprängämnen kan innehålla fett.
- Underlig eller ovanlig lukt.
- Adressetikett eller okänd handskriven adress.
- Ovanlig påskrift eller förtryckta bokstäver med "inskränkande" text, till exempel personligt, privat eller brådskande.
- Avsändare och adress som tyder på önskad anonymitet.
- Överdrivet antal frimärken.
- Tecken på att kuvertet eller omslaget har varit öppnat och sedan återförslutits.
- Oförklarliga metallband, trådar, folie eller liknande.
- Ljud som försändelsen ger ifrån sig, till exempel surrande, tickande eller skvalpande.
- Dykt upp oväntat och oförklarligt, till exempel via en specialleverans med bud eller till receptionen på din arbetsplats.

Hantering av hotbrev

Hantera eventuella hotbrev med försiktighet och förvara dem skyddat så att polisen kan säkra eventuella spår och kan ta del av innehållet för att analysera det.

I de fall du får flera försändelser från samma avsändare är det bra om du bevarar några oöppnade. Analyser kan exempelvis ske genom att studera innehållet i texten och genom att säkra fingeravtryck. Även biologiska spår kan hittas på brevet.

Stalkning - att bli förföljd

I samband med ditt politiska uppdrag eller samhällsengagemang, finns en risk att du blir utsatt för någon som förföljer dig. Detta kan exempelvis ske genom oälkomna telefonsamtal eller påhälsningar, rättshaveristiska brev eller e-post. Men också andra typer av hotfulla handlingar förekommer - som kartläggning via internet och skuggning.

I vardagligt tal kallas olaga förföljelse ofta för stalkning. Men stalkning är ett vidare begrepp som kan innefatta både brottsliga och icke brottsliga handlingar, som kan uppfattas som störande, kränkande eller skrämmande av den som blir utsatt.

Olaga förföljelse innebär däremot att en gärningsperson begår upprepade brottsliga handlingar som måste bestå av ett eller flera av följande brott; misshandel, olaga tvång, olaga hot, hemfridsbrott eller olaga intrång, ofredande, sexuellt ofredande, skadegörelse eller försök till skadegörelse och överträdelse av kontaktförbud.

När någon utsätts för förföljelse är det vanligt att innehållet i till exempel brev och telefonsamtal är hotfullt och aggressivt. Det kan även hända att en person blir förälskad i dig och att detta inte är ömsesidigt, men där den andre inte förstår eller accepterar detta. De upprepade kontakterna kommer då att bestå av inviter och uppvaktning av olika slag, såsom kärleksbrev eller blommor skickade hem eller till arbetsplatsen.

Om du tror att du är förföljd och känner dig hotad av någon är det viktigt att detta anmäls både till polisen och till den säkerhetsansvarige på din arbetsplats eller i din organisation och att det görs en riskbedömning av individen som förföljer eller hotar dig. Riskbedömningen görs av polisen eller Säkerhetspolisen för att bedöma risken för att individen utgör ett hot mot din eller dina anhörigas säkerhet.

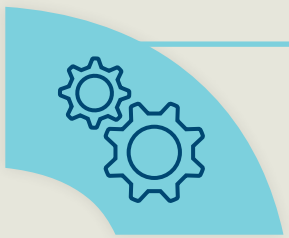
Denna riskbedömning ska göras även om individen uppvisar en sjuklig förälskelse, eftersom det inte är ovanligt att en sådan förälskelse övergår i svartsjuka och hat. Dokumentera alla kontakter som förekommit med individen i fråga, vad som har sagts eller skrivits och hur detta har kommunicerats. Denna information utgör sedan ett viktigt underlag för polis och åklagare.

Det krävs att polis och åklagare gör en bedömning av vilka skydds- och rättsåtgärder som behövs. Detta bör ske i samverkan med den säkerhetsansvarige på din arbetsplats eller i din organisation. Ett juridiskt biträde eller en motsvarande person kan vara ett stöd för dig. Den personen kan även ha möjlighet att medverka i planeringen av skydds- och rättsåtgärder. En kontakt- eller stödperson, till exempel en kollega, bör dessutom utses på din arbetsplats. Du kan mentalt behöva bearbeta det som skett med hjälp av en legitimerad psykolog, psykiater eller annan professionell kompetens med kunskaper och erfarenheter inom området.

Råd vid stalkning

Svara inte på kommunikationsförsök. Varje kontakt innebär en risk för en positiv förstärkning för gärningspersonen och ökar risken för fortsatt oönskad förföljelse och då med ökad intensitet.

Var tydlig med att du inte vill ha någon kontakt med individen ifråga.

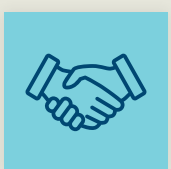


Finns det stödfunktioner som tar emot din e-post eller inkommande samtal måste ett resonemang föras också med de funktionerna om hur ni hanterar hot.

Gör en polisanmälan. Varje gång.

Anmäl till säkerhetsansvariga på din arbetsplats. Gärningspersonen kan komma att försöka ta sig in på arbetsplatsen.

Samla och dokumentera kontakt eller kontaktförsök. Spara all information som styrker hot och trakasserier.



Samarbeta med polis och andra professionella för att få råd kring hur du bör agera.

Rättshaverister

De flesta som arbetar inom offentlig sektor har någon gång varit i kontakt med en rättshaverist och vet att det kan vara svårt att bemöta dessa människor på ett sätt som tillfredsställer deras behov.

Det är viktigt att komma ihåg att bara för att en person är arg och upprörd på myndigheter och politiker innebär inte det att de är rättshaverister. Det kan vara en adekvat reaktion på något som inte fungerar. Man ska också komma ihåg att en person med ett rättshaveristiskt beteende ofta har ett psykiskt lidande som tar sig uttryck i anklagande av andra. De här personerna lägger ned stor del av sin tid på att driva processer, klaga och överklaga och ofta sprider det sig till flera områden. De har en bristande förståelse för att andra människor inte alltid ser eller upplever samma sak som de gör, eller att deras beteende kan påverka andra negativt.

Att bemöta en rättshaverist handlar om att visa empati och värme, samtidigt som man har en tydlig professionell hållning. Ta inga avsteg från de lagar och regler som gäller för verksamheten i syfte att blidka en rättshaverist, då det kan komma att bli en katalysator för ytterligare klagomål och överklaganden i ett senare skede.

Det är viktigt att inte följa med rättshaveristen i dennes tonlägen, utan att istället behålla lugnet och förhålla sig vänlig även om det kan vara svårt. Om ett samtal urartar och blir hotfullt eller kränkande, avsluta samtalet. Ha en handlingsplan för hur ni ska hantera en rättshaverist så att alla vet vad de ska göra och vad de inte ska göra. Om du blir utsatt för en rättshaverist eller annan förföljelse kan det resultera i omständigheter där du tillfälligt kan behöva få alternativa uppdrag eller arbetsuppgifter. Känner du ett behov av det ska du tillsammans med din uppdragsgivare eller ditt parti kontakta polisen eller Säkerhetspolisen för att diskutera eventuella lösningar på problemet. Faktorer som inverkar på bedömningen och de åtgärder som genomförs är om hotet är riktat mot dig som person eller enbart mot din funktion och dina arbetsuppgifter men också hur du och dina närstående upplever situationen. För sådant arbete som kan medföra risk för våld och hot ska det finnas särskilda säkerhetsrutiner.

Ha alltid en hög servicenivå, men till en viss gräns i dessa fall. Vid kontakt - försök behålla lugnet, höj inte rösten, dras inte med i diskussionen och argumentera inte emot. Var saklig och hänvisa till vad du kan göra enligt lagstiftning och rutiner. Visa empati och tydlighet. ”Jag hör vad du säger och förstår hur du ser på saken. Men detta är vad jag kan göra”. Svara på det som efterfrågas, inte mer. Hänvisa till annan om ärendet inte rör ditt område. Förstå att det inte går att förändra personens åsikter. Ifrågasätt inte vanföreställningar. Undvik att svara på upprörda mejl på en gång. Då kan avsändaren hinna lugna sig tills svaret kommer och det hela avdramatiseras. Vid långvarig eller komplicerad kontakt, prova med en annan handläggare eller kollega. En rättshaverist vill ofta avsluta samtalet med ett medskick som är nedlåtande och kritiserande. Låt personen i fråga få sista ordet, kommentera inte ytterligare. Avsluta eller avbryt samtal som blir alltför kränkande, hotfulla eller meningslösa. Det finns gränser.

Utpressning

Det förekommer att personer vill störa den demokratiska beslutsprocessen genom utpressning. Det vanligaste vid utpressning är att någon vill påverka dig att fatta ett avgörande beslut i en känslig fråga. Utpressaren kan använda olika metoder för att tvinga till sig något eller få dig att fatta beslut i en viss riktning. Det kan röra sig om hot mot dig eller någon anhörig.

Ibland kan förtäckta insinuationer räcka för att skrämmas. En utpressare kan utnyttja nedsättande hållhakar eller svagheter hos dig. Ett generellt råd är att ha kontinuerliga samtal med de säkerhetsansvariga i din organisation och uppdatera dem om det sker något i ditt privatliv som kan utnyttjas av någon med onda avsikter. Kontakta säkerhetsansvariga i din organisation om du drabbas av utpressning som är relaterad till ditt uppdrag. Har ni haft återkommande samtal kring din personliga säkerhet får du också bättre råd.

Myndigheter, företag och organisationer i stort, kan också utsättas för utpressning. Motivet är då ofta att störa verksamheten, produktionen eller kommunikationen, men det kan även vara att påverka beslut.

I utpressningsfall kan det förekomma att den som ligger bakom ställer kravet att du inte ska blanda in polisen. Om du hamnar i en sådan situation bör du fundera noga på hur du trots det ska kunna kommunicera med polisen och andra berörda utan att bli upptäckt. I dessa situationer är det viktigt att du håller informationen i en så liten krets som möjligt.

Skydda din identitet och integritet

För den som arbetar som politiker är vardagen till största del fylld av det politiska uppdraget. Oftast kan det utföras som det är tänkt, men det kan finnas element i samhället som vill förhindra eller kartlägga ditt uppdrag.

Den tekniska utrustning som vi använder i allt större utsträckning gör oss också mer sårbara. Intrång och kartläggning kan handla om allt från enskilda personer som är benägna att ta till hot, våld eller trakasserier - till andra stater som vill skaffa sig ett informationsövertag. För att minska risken att utsättas bör du undvika att lämna ut information om dina personliga förhållanden. Risken finns att information om dig kan användas i brottsliga syften. Exempelvis för bedrägerier eller för att utsätta dig eller dina närstående för hot, trakasserier eller angrepp.

Dina personliga uppgifter kan bland annat missbrukas genom att någon kapar din elektroniska identitet, gör oriktiga debiteringar, startar nya abonnemang eller genom förändrad mantalsskrivning.

Någon kan komma åt dina personliga uppgifter genom medlemsmatriklar, adresslistor, webbplatser, e-postlistor, telefonkataloger och via sociala plattformar. Gör därför ett medvetet val kring vilken information du delar med dig av via internet. Använd en stängd profil, det vill säga att din profil endast är synlig för de personer du vill ska se den. Du kan även skapa en separat sida för dig som offentlig person i sociala medier som du håller avskild från din privata sida.

Var också noga med att ofta byta och ha en avancerad inloggning till dina konton. Exempel på avancerad inloggning är så kallade tvåstegsautentisering, som betyder att du behöver ett lösenord och en kod från din mobil eller koddosa för att kunna logga in på ditt konto. →

Personliga uppgifter om dig kan utnyttjas för exempelvis kartläggning eller bedrägeri.

Läs också mer under rubriken ID-kapning på sidan 41.

Läs mer! Det finns guider på internet som beskriver hur man kan få ett grundläggande integritetsskydd. Råden kommer från både tjänsteleverantörer (Apple, Google, LinkedIn) och enskilda skribenter.

Post som du får till din vanliga brevlåda kan i orätta händer användas för att kartlägga dig eller utnyttja dina personliga förhållanden.

Du kan förebygga detta genom att låsa eller förankra brevlådan.

Tänk på att känslig information som inte skyddas kan överhöras eller hamna hos obehöriga personer genom slarv eller okunskap.

Radera inte hot eller trakasserier som du får via e-post eller sms.

Polisen behöver dem i digital form bland annat för att kunna spåra vilken dator de har skickats från.

Räkna med att den information du en gång har lagt ut på internet alltid finns kvar.

Mobiltelefoner och trådlösa nätverk

Mobiltelefoner och surfplattor är idag vanliga verktyg för de flesta av oss. Uppkopplingar som sker från dessa är i de flesta fall säkra (via https://). Men tänk på att offentliga trådlösa nätverk, till exempel på hotell och flygplatser, medför en ökad risk för avlyssning, intrång och kartläggning.

Om ett intrång sker på din bärbara enhet kan det medföra att en obehörig får tillgång till dina uppgifter, det vill säga får en fullständig bild av dina personliga kontakter, din kalender och ditt rörelsemönster samt kan läsa din e-post.

Ett sådant intrång kan också innebära att funktioner i enheten används i ditt namn, exempelvis att det skickas e-post eller läggs ut inlägg på sociala medier som inte du står bakom. För att öka säkerheten kan telefonen och dess innehåll förses med särskild kryptering.

Din mobiltelefon kan lokaliseras med hjälp av ditt telefonnummer. Observera att mobiltelefonen kan lokaliseras även om du har hemligt nummer eller ett så kallat kontantkortsnummer.

Din mobiltelefon kan även lokaliseras med hjälp av trådlösa uppkopplingar (WiFi).

Om WiFi är påslaget på din telefon så söker den aktivt efter nätverk för åtkomst till internet och vid dessa tillfällen annonserar din telefon sig själv. Det finns också appar som automatiskt kontrollerar var din mobiltelefon befinner sig och inkluderar denna position i exempelvis foton, sökningar, webbsidor och uppdateringar på sociala medier.

Kom ihåg att även ditt träningsarmband, din smarta klocka eller din uppkopplade bil kan avslöja din position.

Säkrare hantering av din mobiltelefon:

- Använd kodlås (pinkod) eller ditt fingeravtryck och telefonlås på mobiltelefonen.
- Anslut aldrig till öppna trådlösa nätverk, eftersom din datatrafik då kan övervakas av vem som helst som är på nätverket.
- Om anslutningen till ett öppet WiFi måste ske bör det kombineras med så kallad VPN-anslutning. Se faktaruta nedan.
- Håll telefonen under uppsikt. Lämna den inte till någon obehörig då det finns risk för manipulation.
- Ha inga mobiltelefoner i sammanhang eller rum där särskilt förtroliga eller hemliga samtal förs.
- Ta för vana att alltid stänga av trådlös överföring av data som du inte använder, till exempel Bluetooth (blåtand), eller närfältskommunikation (Near Field Communication, NFC).
- Använd särskilt utvalda telefoner och abonnemang vid aktiviteter som är särskilt känsliga.
- Acceptera inga oväntade program-installationer via e-post, sociala medier, mms eller liknande.
- Använd inga okända minneskort i telefonen.
- Använd antivirusprogram.
- Om din bärbara enhet innehåller känslig information bör du överväga att frångå externa leverantörers erbjudande av säkerhetskopiering av innehållet.
- Kopiera över all information innan du lämnar in din mobiltelefon för service eller uppgradering, genom så kallad total återställning eller Master Reset.
- Glöm inte att regelbundet uppdatera programvaran och apparna i din mobiltelefon.

Risk för avlyssning trots kryptering

Du som är engagerad i säkerhetspolitiska frågor ska aldrig avhandla känslig information via mobiltelefon eller bärbara enheter om de inte har krypton godkända av Försvarsmakten.

I mobilsystem är samtalen vanligen krypterade, men endast mellan mobiltelefon och basstation. Krypteringens styrka kan dock variera och kan även vara avslagen.

Fakta om krypterad förbindelse och så kallad vpn-tunnel:

Virtuellt privat nätverk (VPN) är en teknik som används för att skapa en säker förbindelse, alltså en "tunnel" mellan två punkter i ett icke-säkert datanätverk.

En krypterad internetförbindelse känns igen på att det står https:// istället för http:// i webbläsarens adressfält.

Använder man däremot en app eller en klient (som Outlook) så är det dock andra tekniker som används.

På www.informationssakerhet.se finner du fördjupande fakta om arbetet med att säkra kryptografiska funktioner.


Bibliotek

Offentliga datorer och nätverk

Du bör undvika att använda offentliga datorer eller anslutningar när du handskas med information som du inte vill ska hamna i orätta händer. Om du använder någon annans utrustning, till exempel på hotell, bibliotek eller internetkafé, så ska du utgå från att någon kan komma över dina inloggningsuppgifter eller annan känslig information.

Efter användandet bör du tänka på att ta bort temporära internetfiler från webbläsaren. Om du vill vara extra försiktig kan du även byta lösenord på det e-postkonto du använt på den allmänna datorn. Observera att detta bara är en begränsad åtgärd. Du vet aldrig hur mycket av dina aktiviteter som sparats på en dator som någon annan äger. Utgå från att allt sparas.

Om du ska läsa din e-post ska du se till att det sker på ett skyddat sätt genom säker inloggning och en krypterad förbindelse, det vill säga en vpn-tunnel. Var medveten om att all information du skickar eller tar emot via trådlösa nätverk kan läsas av andra om du inte ansluter på ett säkert sätt.

- Undvik att lämna och förvara teknisk utrustning utan uppsikt, till exempel i bilar, på hotellrum eller på restauranger.
- Var rädd om dina inloggnings-uppgifter till datorn så att ingen obehörig kommer över dem.
- Notera koder och nummer för att kunna spärra abonnemang om något skulle ske.
- Stoppa aldrig in okända usb-enheter eller minneskort i din dator.
- Installera, aktivera och uppdatera kontinuerligt antivirusprogram och personliga brandväggar. Uppdatera också ditt operativsystem och gör säkerhetsuppdateringar regelbundet.
- Stäng av trådlösa nätverk när du inte använder dem.
- Om du använder trådlösa nätverk ska du ändra de ursprungliga inställningarna för till exempel namn och lösenord som leverantören har. Se även till att aktivera den krypteringsfunktion som ingår för att försvåra avlyssning av datatrafik.
- Använd aldrig samma lösenord i privata sammanhang som du använder på arbetet. Välj långa lösenord med blandade versaler, gemener och siffror. De ska inte gå att gissa sig till som exempelvis Hej123 eller Alex1997.

Använd aldrig dina privata lösenord i arbetssammanhang.

ID-kapning

Med ID-kapning eller identitetsintrång menas vanligtvis att någon köper varor eller tar krediter i ditt namn. Ett annat syfte kan vara att använda din identitet på sociala medier och exempelvis sprida falska påståenden i ditt namn. Ha kontroll på dina id-handlingar, var vaksam om någon gör en kreditupplysning på dig och polisanmäl direkt om du misstänker brott.

Skyddade personuppgifter

Uppgifter som registreras i folkbokföringen är som huvudregel offentliga. En eventuell gärningsperson kan alltså med hjälp av uppgifter från folkbokföringen kartlägga en person för att i förlängningen möjliggöra hot eller trakasserier av personen i fråga.

För att uppgifter inte ska missbrukas på detta sätt finns åtgärder som syftar till att skydda hotade personer. Den vanligaste formen av skyddade personuppgifter är sekretessmarkering.

Sekretessmarkering

Sekretessmarkering gör att uppgifter om en enskilds personliga förhållanden skyddas. Det görs om det misstänks att en uppgift ska användas som ett led i förföljelse eller att en enskild eller dennes närstående kan lida skada om uppgiften röjs.

Ansökan om sekretessmarkering görs till Skatteverket. I samband med anmälan ska hotbilden styrkas, till exempel genom att bifoga en kopia på polisanmälan.

Om den enskilde beviljas sekretessmarkering lägger Skatteverket in denna i folkbokföringsdatabasen. Markeringen meddelas andra myndigheter. Markeringen fungerar som en varningssignal till myndigheterna. Den anger att särskild försiktighet ska iakttas vid myndigheternas bedömning av om uppgifter kan lämnas ut eller inte.

Sekretessmarkering är ett bra skydd för den som är utsatt för ett hot, men innan en ansökan sker bör du tänka på att det även komplicerar familjens vardag. Och det finns flera olika avvägningar att ta ställning till. Det kan handla om så praktiska saker som att barnen inte kan vara med på skolfoton eller klasslistor, eller att du själv får svårt att teckna avtal när du köper varor i en affär, eftersom dina uppgifter inte syns i de offentliga registren som butiken har tillgång till.

Avväg också om sekretessmarkeringen bör omfatta samtliga familjemedlemmar så att du inte kan spåras via dessa relationer. Ibland kan det däremot vara en fördel att en av de vuxna i familjen inte är sekretessmarkerad och kan stå för telefonabonnemang och så vidare. Du ska också vara medveten om att sekretessmarkering försvårar, men kan inte helt garantera säkerheten.

En annan sak att tänka på är att själv ta kontakt med bank, post, skola, läkare, föreningar och andra organisationer som inte omfattas av sekretessmarkeringen och be dem skydda dina uppgifter.

Läs mer om bedrägerier på www.polisen.se. Se lagboken (2009:400) om offentlighets- och sekretesslag samt om skydd av personuppgifter under fliken Folkbokföring på Skatteverkets webbplats www.skatteverket.se.

Påverkansoperationer

Vi har ett öppet samhälle med hög teknikнivå. Detta måste värnas. Vi måste samtidigt värna om de svenska politiska beslutsprocesserna. Dessa kan hotas av påverkansoperationer och därför krävs inbyggda skyddsmekanismer och en medvetenhet om att sådana operationer pågår.

Som politisk företrädare kan du behöva hantera ämnen och samhällsfrågor som är av intresse för aktörer utanför landets gränser. Du kan då bli mål för främmande makts påverkansoperationer. Dessa operationer kan bedrivas mot enskilda personer, grupper och hela befolkningar - antingen öppet eller dolt.

Syftet med påverkansoperationer mot Sverige är att påverka vår uppfattning om omvärlden och det som försiggår i vårt land, samt att styra beslutsfattandet i samhället i en viss riktning eller dölja andra viktigare skeenden. Detta sker bland annat genom desinformation och genom att medvetet förvanska hela eller delar av fakta på olika sätt och i olika kanaler. Det kan också handla om att förstärka polariseringen i den offentliga debatten.

Ett högt medietempo, många olika plattformar och i vissa fall resursstarka aktörer gör att information - såväl sann, som falsk eller vilseledande - kan förmedlas brett och snabbt ut i samhället. Idag är det relativt enkelt att skapa en känsla av äkthet, vare sig det gäller informationen som sådan eller plattformen från vilken den sänds.

Kännetecknande för påverkansoperationer är att den ursprungliga avsändaren ofta inte vill avslöja önskat slutresultat, avsikter eller metoder. Det är därför av stor vikt att du kontrollerar den information du nås av för att undvika att du blir en del av en påverkansoperation.

Ett sätt att minimera risken för att utsättas är att vara medveten om att påverkansoperationer pågår, det vill säga att det finns aktörer som vill påverka svenska beslutsfattare i en viss riktning. Ett viktigt förfarande för att begränsa effekterna är att vara källkritisk - att finslipa din förmåga att avgöra äktheten i informationen eller hos avsändaren.

Det behöver understrykas att påverkansoperationer också bedrivs genom att verkligheten manipuleras, det vill säga att en viss typ av agerande framkallas med exempelvis hot eller mutor. Syftet med ett sådant agerande kan vara att få till exempel politiker eller journalister att uttala sig om en sådan framtvingad händelse. Ett skydd mot denna typ av påverkan är att undvika att kommentera en händelse innan bekräftad information är tillgänglig.

Syftet med påverkansoperationer mot Sverige är att påverka vår uppfattning om omvärlden.

Personliga möten i syfte att värva

Statliga aktörer, både individer som arbetar på uppdrag av en annan stat, eller organisationer som är knutna till dessa, har resurser. De använder sig av bland annat så kallade underrättelseofficerare, vars uppdrag är att bedriva påverkan med hjälp av personliga möten, exempelvis under täckmantel som diplomat eller journalist. Denna metod är effektiv men kräver ett visst mått av förberedelser, som kartläggning av målobjektet och åtgärder för att skydda operationen. Denna typ av verksamhet pågår dagligen i Sverige.

Du bör känna till att statliga aktörer ofta arbetar långsiktigt. Du som är politiskt aktiv kan exempelvis tidigt i din karriär ha blivit bekant med någon som många år senare söker upp dig eller agerar som om ni av en tillfällighet råkar stöta på varandra. Mötet kan naturligtvis vara äkta och utan några baktankar, men om denna person efter en tids återupptagen kontakt i detalj börjar intressera sig för dina politiska uppdrag och information du eller någon nära dig har, bör du bli misstänksam. Du kan vara utsatt för så kallad kultivering, en fas i en långsiktig plan där främmande makts utsände söker vänskapsband med någon för att få denne att lämna ut upplysningar som kan ge dem ett informationsövertag.

Det yttersta målet kan vara att du ska bli värvad och via betalning eller genom andra förmåner ska fortsätta ge ut information. Om du misstänker att du är utsatt för ett värvningsförsök ska du kontakta Säkerhetspolisen.

Läs mer om hur värvning kan gå till i Säkerhetspolisens årsbok.

sakerhetspolisen.se

Säkerhet i bostaden och vardagen

En viktig del i att skapa trygghet är att känna sig säker i sin bostad eller på andra platser där du regelbundet vistas, exempelvis hos din särbo eller i ett fritidshus.

Ett första råd är att be grannar som du litar på att hålla ett öga på din bostad om du är bortrest. Ett annat råd är att ha ett så kallat skalskydd, det vill säga att säkra de vanligaste intrångsvägarna:

- Entrédörrar.
- Fönster som lätt kan nås från marknivå eller från tak på utbyggnader.
- Fasadmonterade brand- och utrymningsstegar som kan användas som hjälpmedel för att ta sig förbi skalskyddet.
- Takluckor.

Om du lever under hot bör du planera för alternativa utrymningsvägar i ditt hem. Beroende på hur hotsituationen ser ut kan din organisation eller annan kvalificerad personal och i särskilda fall lokal polis, bistå med säkerhetsrådgivning. Rådgivningen kan belysa specifikt hur skyddet i bostaden eller på arbetsplatsen kan förbättras eller beröra hur du ska förhålla dig till din närmiljö. Här följer en del av de råd som brukar ges.

- Dörrarna till din bostad bör ha en skyddsnivå som motsvarar inbrottsskyddade dörrar enligt gällande standard.
- Se till att fönster, balkong- och terrassdörrar som kan nås från markplanet har samma skyddsnivå som entrédörrarna.
- Montera en dörrkik på entrédörren. Via vidvinkelfunktion kan du upptäcka faror och identifiera personer utan att öppna dörren. Undvik insyn med ett skydd över dörrkiken på insidan av dörren.
- Ha god belysning utanför dörrar, vid uppfarten och i trädgården om du bor i hus.

Dörrar och brevinkast

Om du bor i lägenhet är en säkerhetsdörr med extern förstärkt brevlåda det bästa skyddet. Om du har ett brevinkast i ytterdörren kan en förebyggande åtgärd vara att montera en säkerhetsbrevlåda med brandskydd på insidan av dörren. Istället för brevinkast kan du ha en utvändigt låsbar brevlåda eller en postbox. Du som bor i hus bör ha en brevlåda med lås.

Ha god belysning utanför dörrar, vid uppfarten och i trädgården om du bor i hus.


SET KEY

Fönster och glasade ytor

Om du bor i villa, undvik att ha glasade partier i eller vid sidan om entrédörren. Om det finns glasade partier kan dessa förses med skyddsglas eller galler. För att skydda fönster kan du montera en speciell plastfolie på insidan av glaset som ger ett visst inkastskydd och insynsskydd.

Nycklar, kort och koder

Nycklar, inpasseringskort och portkoder kan utnyttjas för att komma förbi skalskyddet till din bostad. Skydda dessa så att de inte kommer i orätta händer. Om du tappar bort nycklar, inpasseringskort eller koder är det viktigt att du omedelbart meddelar din hyresvärd eller bostadsrättsförening. Det kan dessutom gå att lista ut vilka siffror som ingår i kombinationerna för olika knappsatser och displayer med ledning av smuts- och fettfläckar eller kemikalier som är avsedda för detta ändamål. Byt därför kod och rengör knappsatsen regelbundet.

Saker att tänka på:

- Håll bostadsnycklar åtskilda från andra nycklar.
- Se till att nycklar, kort och koder inte kan identifieras som dina.
- Byt låscylindrar om nycklar kommit på avvägar.
- Förvara inte nycklar på platser som lätt kan upptäckas eller kopplas samman med dig.
- Lämna aldrig ifrån dig nycklar till någon du inte litar på. Tänk på risken att nycklarna kopieras.
- Byt lås om du byter bostad.

Lämna aldrig ifrån dig nycklar till någon du inte litar på, då det medför en risk att nycklarna kopieras.

Familj – skyddet för närstående

En förövare kan pröva att gå via din familj för att försöka påverka din förmåga att fungera i ditt politiska uppdrag. Genom medvetna val och råd från säkerhetskunniga kan ni tillsammans bygga trygghet. Samtliga familjemedlemmar bör vara införstådda i en eventuell hotsituation och känna till de åtgärder som görs.

Kanske har du och din familj redan en policy om vad ni i familjen exponerar på sociala medier. Exempelvis vilken sorts statusuppdateringar ni gör, vad ni exponerar för innehåll och foton. Tänk igenom den regelbundet. Se vidare kapitlet om sociala medier sidan 18.

Saker att tänka på:

- Lämna inte ut uppgifter om förhållanden i hemmet som kan påverka säkerheten, eller om var personer i familjen uppehåller sig.
- Uppge inte telefonnummer eller adress vid felringning.
- Be exempelvis servicetekniker, hantverkare eller bud att visa legitimation innan du tar emot någonting från dem.
- Var uppmärksam på okända personer som rör sig på ett oförklarligt sätt i närområdet eller söker kontakt med er på arbetsplatsen, i skolan eller under en fritidsaktivitet.
- Var försiktig med gåvor från okända.

Lär barnen agera rätt

Om det finns en hotbild mot dig och din familj bör du informera exempelvis personal vid förskola och skola samt ledare inom fritidsaktiviteter. Instruera barnen i hur och när de ska larma nödnumret 112. Du kan också uppmärksamma barnen på att vara försiktiga genom att:

- Kontrollera besökare till bostaden genom dörrkik eller fönster.
- Inte släppa in okända personer i bostaden eller trappuppgången.
- Vara vaksamma mot kontaktsökande personer, inte följa med eller ta emot gåvor från okända.
- Gå tillsammans med en kamrat eller vuxen, till och från skolan och olika fritidsaktiviteter.
- Meddela alla förändrade tider, till exempel hämtning från skolan och fritidsaktiviteter.

Samtliga familjemedlemmar bör vara införstådda i en eventuell hotsituation och känna till de åtgärder som görs.

Larm och skyddsåtgärder

Förutom det självklara att ha brandvarnare, så finns en rad olika larm - både fasta och mobila - som du kan använda för att skydda dig och din bostad.

Inbrottslarm

Ett inbrottslarm kan med fördel installeras i din bostad som en extra skyddsåtgärd. Bor du i hus bör entrédörrar, glasade partier och garage skyddas av inbrottslarmet. Larmet kan vara ett ljudande larm, en siren eller ett tyst larm som överförs till en larmcentral. Idag kan de flesta övervakade larm kompletteras med rökdetektorer vilket skapar en högre skyddsnivå vid bränder.

Överfallslarm och personlarm

De flesta politiker känner sig trygga i sin vardag. Men för den som är, eller riskerar att bli, utsatt för hot, våld eller trakasserier kan det vara motiverat att ha ett överfallslarm eller personlarm.

Överfallslarm kan vara ett fast installerat larm i din bostad eller ett bärbart överfallslarm. Dessa ger ifrån sig ett högt ljud för att göra din omgivning uppmärksam på att någon försöker angripa dig och samtidigt skrämma bort denne. Larmen finns i olika utföranden och i en nödsituation kan de genom en enkel knapptryckning sända viktig information till en larmcentral. Det kan krävas att du tar en personlig kontakt med larmcentralen för att säkerställa din position och larmets GPS-funktion.

Olika former av bärbara överfallslarm tillhandahålls av larmoperatörer, bevakningsbolag och andra branschföretag.

På marknaden finns också personlarm som används via mobiltelefon. Dessa är i första hand tänkta att larma en närstående eller en kollega. Larmen brukar kombineras med en personlig webbsida där bland annat positionen presenteras grafiskt. Mer information hittar du om du söker på ”trygghetslarm mobiltelefon gps” på internet.

Rådgör med säkerhetsansvariga om du har behov av överfalls- eller personlarm, och glöm inte att ha larmet med dig.

Inbrottslarm

Anpassa larmet utifrån din boendemiljö för att minimera risken för onödiga larm och därmed även oönskade insatser från bevakningsbolag eller polis. Det vill säga anpassa systemet utifrån om du exempelvis har barn eller husdjur.

De flesta system har alternativa överföringsvägar. Det betyder att även om larmöverföringen störs ut kan larmet ändå fungera via bredbandsuppkoppling (fiber, ADSL) eller motsvarande.

Fundera på vilka skydds-åtgärder du ska vidta om du befinner dig i bostaden när larmet går, oavsett om det sker på dagen eller natten.

Larmmottagning bör ske till en dygnet-runt-bemannad och godkänd larmcentral.

Inbrottslarm kan med fördel kompletteras med överfallslarm och rökdetektorer.

Var försiktig med att använda fjärrkontroller för att styra ditt larm. Risken finns att någon obehörig kommer över fjärrkontrollen och kan larma av.

Sätt upp en skylt om bevakning eller larm, det kan vara avskräckande.

Elektroniska ytterlås är en relativt ny teknologi. Kontrollera därför att de är godkända av ditt försäkringsbolag.

Larma med mobil

I nödsituationer kan du normalt sett larma 112 även om telefonnätet eller ditt SIM-kort inte fungerar. Om du ringer 112 utan SIM-kort eller blir roamad till ett nät som du normalt inte har tillgång till visas inte telefonnumret för SOS-alarm.

Du kan också lägga in 112 som snabbval eller kortnummer i din mobiltelefon för att snabbt kunna larma i en eventuell nödsituation.

Ett flertal mobiltelefoner är utrustade med nödlägesfunktioner där position och nödsignal kan sändas till en förprogrammerad mottagare med en enkel knapptryckning. Om det inte är aktuellt med ett formellt överfallslarm kan det öka den personliga tryggheten att känna till dessa funktioner i mobilen samt öva på att använda dem.

Larma med hemligt telefonnummer

Om du har hemligt telefonnummer på din mobiltelefon kan det begränsa möjligheten och försvåra – eller hindra – identifieringen av dig när du larmar exempelvis polisen via 112. Du kan komma fram men det går inte att se ditt telefonnummer. För att komma förbi detta kan du identifiera dig genom att använda ett prefix före larmnumret. Faktarutan nedan visar hur du gör.

ICE visar anhörigas telefonnummer

Du kan underlätta för räddnings- och sjukvårdspersonal att komma i kontakt med anhöriga eller andra kontakter i händelse av sjukdom eller olycksfall där du inte själv kan lämna information. Det kan du göra genom att lägga in en post under kontakter i mobiltelefonens adressbok och kalla den ICE. Posten ICE (In Case of Emergency) används internationellt och kan innehålla telefonnummer till ett valfritt antal personer, till exempel anhöriga och arbetsgivare, som du vill ska meddelas om något allvarligt händer dig.

ICE

På nyare mobiltelefoner finns möjligheten att lägga till ICE-kontakterna så att de går att komma åt även om telefonens knapplås är aktiverat.

Programmera in ditt larmnummer med prefixet *31# i din mobiltelefon, till exempel *31#07XXXXXXX
Olika lösningar gäller för olika teleoperatörer. Hör efter vad som gäller för din.

Anmäl alla hot

Om du trots förebyggande åtgärder för din säkerhet, blir utsatt för hot, våld eller trakasserier finns det flera saker du ska göra.

Till att börja med är det viktigt att du polisanmäler alla hot. Det är en markering att du inte accepterar det du blivit utsatt för. I och med en anmälan kan också polisens brottsoffer- och personsäkerhetsarbete inledas. En anmälan underlättar också polisens underrättelsearbete. Även i de fall där en anmälan inte kan knytas till en gärningsperson, så kan anmälan vara en viktig pusselbit för att analysera liknande brott och tillvägagångssätt.

Om du misstänker att det finns en koppling till din yrkesroll och ditt politiska engagemang bör du informera om detta när du gör en polisanmälan. Polisen kan, under vissa förutsättningar, åtkomstskydda din anmälan för att öka sekretessen kring den och på så sätt avgränsa vilka som kan läsa anmälan. Ofta kan då även anmälningsupptagaren redovisa så lite som möjligt i anmälan och istället välja att skriva en mer utförlig bilaga.

I samband med polisanmälan får du information om lämpligt brottsofferstöd och vad du själv kan göra för att skydda dig och dina närmaste. Om du har en hotbild mot dig gör polisen en skyddsplan och planerar eventuella skyddsåtgärder i dialog med dig.

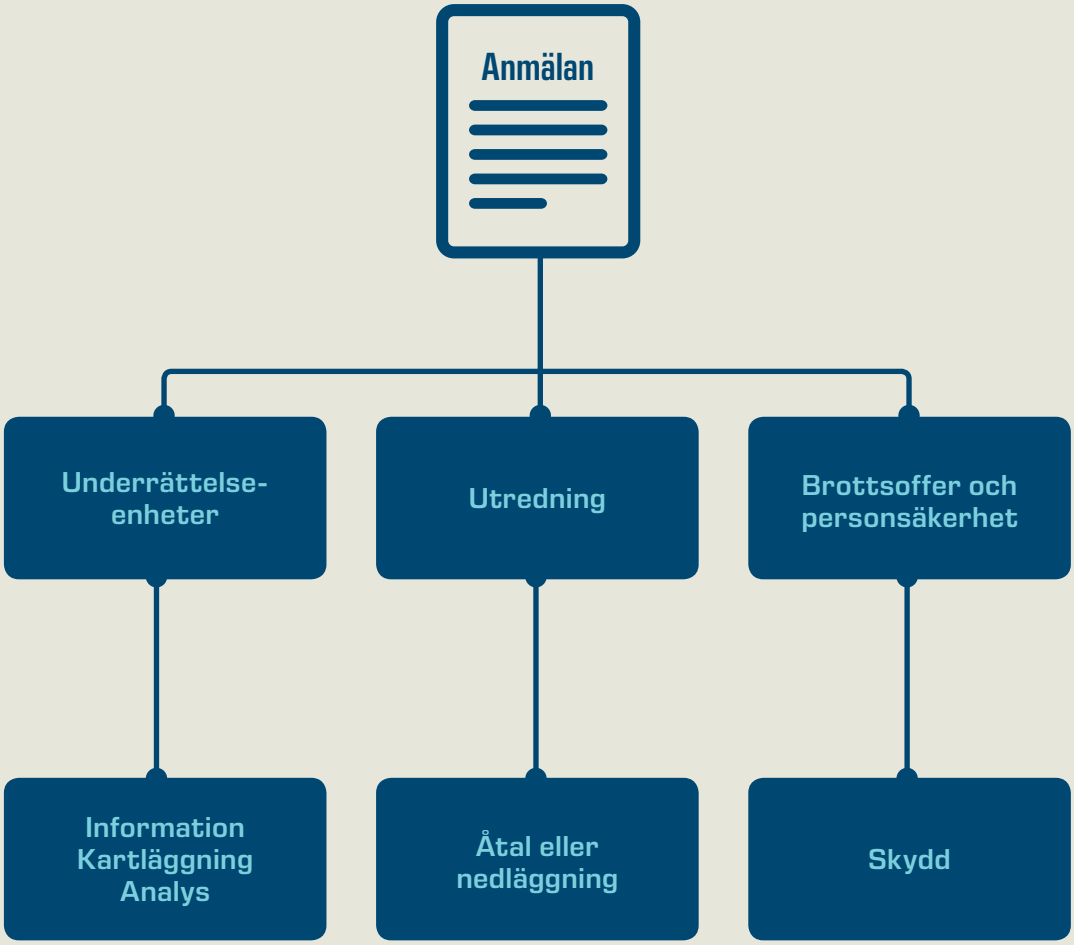
Det är polisen och Åklagarmyndigheten som fattar beslut om åtgärder i samband med misstanke om brott. Under en brottsutredning omfattas uppgifter som kan innebära skada eller men för de inblandade individerna eller för utredningen i sig, av sekretess.

I vissa fall pågår brottsutredningen parallellt med polisens skyddsarbete och kan leda till att en gärningsperson identifieras, åtalas och döms. I andra fall saknas möjlighet att bedriva utredningen framåt och förundersökningen läggs ned, men då kan polisens skyddsarbete ändå fortsätta och du kan istället fokusera på ditt politiska uppdrag.

Skyddsarbetet är med andra ord inte avhängigt om man har identifierat en gärningsperson eller inte, utan utformas efter det behov som finns. Det är därför viktigt att göra en polisanmälan eftersom skyddsarbetet kan påbörjas i och med att anmälan har upprättats.

Dokumentera och spara sådant som har anknytning till brottet då det kan underlätta polisens utredning. Informera även säkerhetsansvariga på din arbetsplats eller din närmaste chef om det inträffade.

Detta sker vid en polisanmälan



Kontaktförbud

Ett exempel på en åtgärd som kan ske efter en polisanmälan är kontaktförbud. Det innebär normalt att någon som hotar eller trakasserar dig förbjuds att besöka och ta kontakt med dig.

Förbudet kan utvidgas till att personen som hotar dig inte får vara i närheten av din bostad eller arbetsplats. Syftet med kontaktförbudet är att undvika situationer som kan bli farliga. Att överträda ett kontaktförbud är brottsligt och kan leda till böter eller fängelse upp till ett år. Kontaktförbudet är tidsbegränsat.

Om du vill ansöka om kontaktförbud ska du vända dig till polisen. De kan också svara på frågor.

En åklagare eller en domstol beslutar om kontaktförbud. Frågan om kontaktförbud kan tas upp även om du inte uttryckligen begärt det.

- **Kontaktförbud** innebär att den förbudet avser inte får besöka, kontakta eller följa efter den skyddade personen.

- **Utvidgat kontaktförbud**, innebär att den förbudet gäller, inte får besöka eller vara i närheten av den skyddade personens bostad, arbetsplats eller andra ställen där hon eller han brukar vara.

- **Särskilt utvidgat kontaktförbud**, innebär att den förbudet gäller inte får vistas i ett större område runt den skyddade personens bostad, arbetsplats eller andra ställen där hon eller han brukar vara. Denna typ av kontaktförbud förutsätter att den som ansöker sedan tidigare har ett utvidgat kontaktförbud som överträtts genom fysisk överträdelse.

Normalt ska ett särskilt utvidgat kontaktförbud förenas med elektronisk övervakning, vilket innebär att förbudspersonen får bära en elektronisk fotboja som larmar om han eller hon överträder förbudsområdet eller inte sköter sin utrustning.

Att överträda ett kontaktförbud är brottsligt.

Läs mer i lagen (1988:688) om kontaktförbud.


HOLD THE HANDRAIL
AND YOUR LUGGAGE

Resor – inrikes och utrikes

Biljetter bokas, resväskor packas, rätt dokument ska med.
I det politiska arbetet rör sig många både i och utanför Sverige.

En del reser ofta, andra mer sällan. Det är ovanligt med allvarliga hotsituationer vid resor, men de senaste årens terrorattacker har skapat en större medvetenhet om säkerheten i samband med resor.

Om du känner oro för att utsättas för angrepp i någon form under din resa ska du tänka på att välja en trygg omgivning och förbereda dig så att du har en alternativ handlingsplan. Det ska du göra oavsett om du reser inom landet eller utomlands och oavsett om du tar dig fram till fots eller reser med bil, buss, tåg, tunnelbana eller flyg.

I samband med resor befinner du dig ofta i nya miljöer. Då du exempelvis besöker restauranger bör du vara uppmärksam på hur du kan ta dig ut via annan utgång än entrén. Välj om möjligt en plats långt in i lokalen med uppsikt över rummet. Försök bedöma din omgivning och människor i din närhet.

Saker att tänka på:

- Om du känner dig otrygg, res inte ensam.
- Lägg in nödnumret 112 eller det nödnummer som är aktuellt i det land där du befinner dig som snabbval i din mobiltelefon så att du snabbt kan larma.
- Undvik att informera okända personer om var, när och hur du reser.
- Informera anhöriga om vart du ska resa, när och hur samt hur du kan nås. Glöm inte att meddela om det blir några förändringar så att du kan nås snabbt.
- Om du ska iväg på en längre resa kan det vara bra att be någon du litar på att se efter din bostad.

Vid resa ska du alltid informera anhöriga om vart och när du ska resa och hur de kan nå dig.

Konfliktdrabbade områden

Riskerna vid en utlandsresa eller utlandstjänst varierar mellan olika länder och även mellan olika orter inom ett land. Tillfälligt uppkomna politiska situationer i landet kan också förändra förhållandena.

Innan du reser behöver du uppdatera dig om läget. Konflikter i landet eller situationer i omvärlden kan påverka din säkerhet också under resan. Se till att ha en alternativ plan om det oförutsägbara skulle inträffa.

Bedöm om det är lämpligt att du åker och vilka eventuella skyddsåtgärder du bör vidta för att minska riskerna på plats. Denna bedömning bör du göra i samråd med din organisation eller säkerhetsansvariga på din arbetsplats.

Ha en plan för hur du tar dig därifrån om något händer. Innan du åker bör du också enligt era rutiner informera berörda på din arbetsplats och anhöriga om:

- Vart du reser och om ditt boende.
- När du ska vara framme och när du beräknar att vara tillbaka.
- Hur du kan kontaktas.
- Hur du ska resa och vilka aktiviteter och programpunkter du har planerat, särskilt om de är kontroversiella.
- Vem eller vilka du ska träffa.

Risker vid flygresor

När du ska resa utomlands med flyg finns det en del saker att tänka på. Under resan bör du vara uppmärksam på din omgivning och hålla ditt bagage under noggrann uppsikt. Den som vill kartlägga någon vill komma över information. Det kan vara fakta, men också kontakter eller samverkanspartners du har.

Utifrån deras perspektiv finns arenor där det är lätt att överhöra samtal eller komma över papper eller datorer. Exempel på sådana platser är flygplan och flygplatser, men även på bussar och tåg, konferenser, mässor och i hotellreceptioner. Lämna en detaljerad resplan till dina anhöriga och din arbetsgivare och meddela dem snarast om eventuella avvikelser.

- Undvik helst att boka en resa med byten i högriskländer.
- Undvik att anlända till resmålet mitt i natten eftersom det kan vara svårare att få taxi eller annan hjälp samt att risken för kriminalitet är större.
- Var på plats i god tid innan avresan på grund av den ökade säkerheten på flygplatser.
- Undvik att spendera för mycket tid i vänthallen innan du har passerat säkerhetskontrollen då risken för attentat är avsevärt högre där.
- Undvik att använda hörlurar på flygplatser då du kan gå miste om viktig information samt få eventuell förvarning vid en incident. Samma råd gäller under färd med allmänna kommunikationer vid förhöjd terrorhotnivå.
- Minska risken för exponering genom att packa rätt så att du inte får problem i säkerhetskontrollen. Välj en väska utan fickor på utsidan då någon kan placera något föremål i den.
- Lämna aldrig ditt bagage till någon annan eller utan uppsikt – från packning till incheckning.
- Ha inte någon utvändig märkning med anknytning till ditt arbete om det kan vara känsligt, till exempel din organisations eller ditt partis emblem på bagage, kläder, väskor eller liknande.
- Ha gärna med dig en kopia på passhandlingen och extra foton, och förvara dem åtskilda från passet. Om du förlorar ditt pass kan kopian och fotona användas som stöd när du ska identifiera dig och ordna med ett nytt pass.

Transfer från flygplatsen

Vid utlandsresor har du som politiker ofta en organisation eller annan motpart som bjudit in dig och möter dig vid flygplatsen. Oavsett om de har en egen bil eller om ni ska åka taxi så ska du säkerställa att dörrarna är låsta vid färd. Var inte rädd för att be chauffören dra ner på farten om det går för fort. Trafiken är den absolut största risken du utsätter dig för.

Om du blir hämtad av chaufför:

- Se till att du fått chaufförens namn och nummer i förväg.
- Lämna även ert eget nummer till mötande part så att eventuella förseningar kan meddelas och för att minimera tiden i ankomsthallen och på parkeringsområdet.
- Chauffören kan vara en god källa till information om det aktuella säkerhetsläget.

Taxiresor

Ta reda på vilka taxibolag som är tillförlitliga. Undvik så kallade friåkare. Åk aldrig taxi med någon som har okända ”medpassagerare”. Ha gärna en utskrift på hotell och destination för att undvika missförstånd. Använd alltid bälte. Om dessa saknas, byt bil. Betala taxifärden i bilen. Känns resan obehaglig, ring gärna din kollega eller en partnerorganisation och meddela att ni är på väg. Fråga chauffören när ni beräknas vara framme. Håll samtalet igång så länge det behövs.

Säkerhet på hotellet

När du bokar hotell ska du välja ett säkert boende där du kan känna dig trygg, hör exempelvis med kolleger om någon av dem varit på platsen tidigare. Här följer några råd som kan vara relevanta.

Överväg om det är nödvändigt att lämna ut din e-postadress vid incheckning. En sådan trivial sak som att nämna sitt rumsnummer kan vara av intresse för någon som kartlägger dig. Undvik att bo på markplan, eftersom det kan öka risken för inbrott. Tänk också på att från våningsplan sex är det mer komplicerat att bli räddad vid en brand.

Studera utrymningsplanen för hotellet och ta reda på var de närmaste nödutgångarna finns. Ta reda på om det finns en återsamlingsplats. Att hänga ut skylten ”stör ej” och låta tv:n vara på kan hålla en inkräktare borta. Lämna inte känslig information som rör ditt arbete, din person eller din familj på hotellrummet.

Ta för vana att låsa in värdehandlingar så som pengar, pass, id-kort, mediciner, datorer och arbetsmaterial i ett säkerhetsskåp. Gör en bedömning av förvaringsskåpen för värdesaker innan du nyttjar dem.

Precis som i vanliga fall ska du undvika att lägga ut olämplig information på sociala medier. Den politiska situationen eller det lokala sammanhanget kan dessutom ha betydelse för hur dina kommentarer uppfattas.

Ta för vana att alltid låsa in dina värdehandlingar i säkerhetsskåpet.

Allvarliga händelser utomlands

Att svenska medborgare i utlandet utsätts för utpressning eller hamnar i gisslansituationer sker ytterst sällan. Men det kan hända och ställer stora krav på uthållighet, kunskap och förmåga att hantera den uppkomna situationen.

Om du ska resa till ett så kallat högriskland bör du ta råd av säkerhetsansvariga och gå igenom de råd som ges av Utrikesdepartementet. Nedan finner du en del av dessa:

Ha med dig telefonnummer till den svenska ambassaden eller konsulatet i landet för att få råd och hjälp om du hamnar i en nödsituation. Om det saknas svensk representation i landet kan du vända dig till ett annat nordiskt lands eller EU-lands ambassad eller konsulat.

Informera dina anhöriga om du reser till ett land med dålig mottagning. Uppdatera dig kontinuerligt om händelser som rör staden eller platsen och politiska händelser i världen som kan påverka säkerheten där du befinner dig.

Undvik situationer som ökar risken för att bli utsatt för till exempel rån eller kidnappning. Dessa brott är ofta kopplade till den kriminella situationen i ett land, och du bör därför informera dig om hur det ser ut i det land du ska åka till.

Risken för att bli utsatt kan vara något högre vid besök på vissa restauranger, hotell eller lokaler, speciellt i länder med pågående konflikter. Exempelvis kan platser där många befinner sig samtidigt, som vid en högtid eller ett event, vara en måltavla för terrordåd.

Var observant i den miljö du befinner dig så du kan upptäcka och undvika tänkbara riskmoment.

Var förutseende och ha medicin eller recept lättillgängliga om du lider av en sjukdom. Detta kan minska din sårbarhet vid hastigt uppkomna situationer. Ha med dig aktuella telefonnummer till anhöriga, arbetsgivare och försäkringsbolag.

Resor till vissa länder kräver fler säkerhetsåtgärder än andra. Gå igenom de råd som ges av Utrikesdepartementet.

Du kan ringa 112 vid nödsituationer inom Europa och genom ett flertal andra GSM-nät utanför Europa. Du kan också ringa larmcentralerna SOS International på telefon +45 70 10 50 50 eller Euro-Alarm på telefon +45 70 10 90 50. Spara dessa nummer i telefonboken.

Ärenden som berör svenska medborgare i utlandet hanteras av särskilt utbildade förhandlare på polisens Nationella operativa avdelning (Noa) i samverkan med Utrikesdepartementet samt utländska myndigheter och organisationer.

Läs mer! På Utrikesdepartementets webbplats hittar du reserekommendationer som innehåller råd för olika länder när det gäller till exempel säkerhets- och hälsoläget i landet eller information om olika krissituationer. Reserekommendationerna hittar du på www.regeringen.se, sök under UD och reseinformation. Eller ladda ner appen: UD Resklar.

Terrorangrepp och andra attentat

Under senare år har attentat i form av politiskt eller religiöst våld i västvärlden ökat. Sannolikheten att drabbas är liten, men det är ändå viktigt att känna till hur du bör agera om ett terrorangrepp eller motsvarande våldsbrott skulle inträffa.

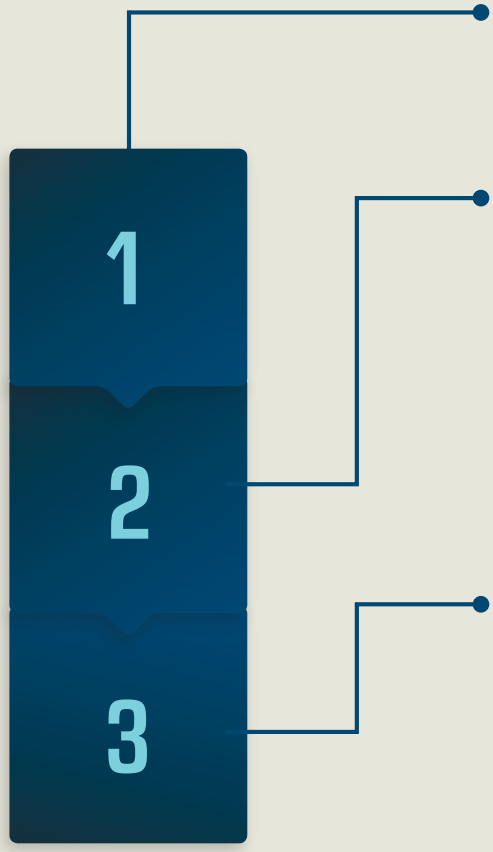
Ett sätt att vara mentalt förberedd är att föreställa sig olika scenarier och situationer, och hur du skulle agera i dessa. Den mentala förberedelsen kan vara avgörande eftersom den tid det tar att förstå vad som händer kan vara vital för om du tar dig ur situationen eller inte.

Om du rör dig i offentliga eller andra publika miljöer där ett dåd kan ske, bör du vara uppmärksam på nödutgångarna. Ett annat råd är att inte avfärda oljud som om de vore smällare. När oväntade händelser inträffar är det många som först ser hur andra reagerar innan de själva gör något. Var inte den personen. Ta initiativ och agera.

En annan situation som kan uppstå är att någon eller några med onda avsikter tar sig in i ett kommunhus, socialkontor, skola eller andra offentliga byggnader. Se till att ha en handlingsplan för en sådan situation, den ska innehålla förslag på utrymningsvägar och möjligheter att blockera eller låsa lokaler.

Se till att ha en handlingsplan för om någon med onda avsikter tar sig in i er byggnad.

Tre steg vid terrorattentat



1. Fly

- Ta för vana att i nya lokaler alltid notera nödutgångar.
- Fly från platsen och sätt dig själv i säkerhet.
- Allmänheten och du själv är måltavla.
- Var förberedd på att ytterligare attentat kan ske.

2. Sök skydd

- Om du inte kan fly ska du gömma dig på en plats du bedömer vara säker. Sök ett utrymme som går att låsa eller blockera. Undvik fönster och dörrar tills faran är över.
- Lås, släck ljuset och var tyst.
- Slå av ljudet på din telefon.
- Ring inte i onödan till personer som kan befinna sig i riskområdet, du kan utsätta dem för fara.
- Lämna inte ett säkert område för att se vad som händer. Gå inte tillbaka förrän du förvissat dig om att polisen har gjort platsen säker.
- Var alltid beredd på en ny attack och följ de råd som polis och räddningstjänst ger.

3. Larma

- Ring/larma 112 så fort du får möjlighet.
- Det är polisens uppdrag att avbryta ett pågående attentat. För att polisen ska kunna komma till platsen krävs att de får information om händelsen.
- I en allvarlig situation med stor förödelse blir ofta telefonnätet överbelastat och det kan då vara svårt att komma fram. Även om samtal inte kopplas fram kan datameddelanden nå fram.
- Följ myndigheternas - och särskilt polisens - uppmaningar. När polisen kommer till platsen, se till att du inte kan misstas för att vara gärningsman. Håll därför inget i händerna.

Läs mer på polisens webbplats
www.polisen.se. Där får du generella råd om hur du ska agera vid ett terrorattentat eller motsvarande våldsbrott.

Vid större samhällshotande händelse
se alltid: www.krisinformation.se

Dessa råd bygger på de samlade riktlinjer som svenska myndigheter enats om våren 2018.

Säkerhet byggs tillsammans

Säkerhetspolisens uppdrag är att skydda Sverige och vår demokrati. Det gör vi genom att se till att var och en fritt kan utöva sina demokratiska rättigheter.

Du som är politiskt aktiv ska kunna utöva dina uppdrag på ett säkert sätt. Du ska kunna röra dig fritt och ha nära kontakt med de människor du representerar. De medvetna val du och din organisation gör i er vardag är en vital del i det säkerhetshöjande arbete vi ständigt måste utföra tillsammans. Detta har varit utgångspunkten för de råd som handboken Personlig säkerhet ger.

Boken är primärt skriven för politiskt aktiva, men råden fungerar lika väl för andra utsatta yrkesgrupper.

Säkerhetspolisen har tagit fram boken i nära samarbete med Polismyndigheten.

Hela denna bok finns även att ladda ner på:

sakerhetspolisen.se

Box 12312, 102 28 Stockholm
Tfn 010-568 70 00, fax 010-568 70 10
E-post sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se