# Personlig säkerhet

Säkerhetspolisen

Säkerhetspolisens uppdrag är att skydda Sverige och demokratin. En grundläggande del i det är att den centrala statsledningen kan utföra sitt uppdrag under trygga och säkra former.

# Innehåll












# Säkerhet byggs tillsammans

Säkerhetspolisens uppdrag är att skydda Sverige och demokratin. Så att det som inte får hända, inte heller händer. En grundläggande del i demokratin är att den centrala statsledningen ska kunna utföra sitt uppdrag under trygga och säkra former. Samtidigt uppger var fjärde förtroendevald att de utsatts för trakasserier, hot eller våld under 2020*, och hotbilden mot Sverige har breddats och blivit mer komplex.

Hotet från främmande makt utmanar våra demokratiska värden. Varje dag sker försök att stjäla uppgifter av betydelse för Sveriges säkerhet eller att påverka svenskt beslutsfattande. Sammantaget innebär det breddade hotet att både grundläggande fri- och rättigheter och vårt politiska oberoende hotas.

**Säkerhetspolisens uppdrag** är att säkra framtiden för demokratin. Det gör vi genom att avvärja hot mot Sveriges säkerhet och medborgarnas fri- och rättigheter. Tillsammans med Polismyndigheten arbetar vi för att våra politiker i regering och riksdag ska ha möjlighet att utföra sina uppdrag utan att utsättas för hot eller våld.

**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 Sveriges demokrati om folkvalda politiker inte vågar fatta beslut på grund av upplevt obehag eller faktiska hot och trakasserier. I den här handboken är politikers säkerhet därför i fokus och råden ska ses som ett stöd i arbetet. Säkerhetspolisens mål är att öka säkerhetsmedvetandet och tryggheten för politiker inom den centrala statsledningen. På så sätt bidrar vi till att säkra det demokratiska systemet.

**I handboken Personlig säkerhet** ges exempel på förebyggande åtgärder och säkerhetsåtgärder som kan användas för att förhindra eller avstyra hotfulla situationer om de skulle uppstå. Här behandlas allt från sociala medier till säkerhet i hemmet och resor utomlands. Boken är primärt skriven för den centrala statsledningen, men råden fungerar lika väl för andra politiskt aktiva och andra utsatta yrkesgrupper och personer.

** enligt Brottsförebyggande rådets "Politikernas trygghetsundersökning 2021".*

# Säkerhet vid politiskt arbete

Det finns aktörer som vill begränsa den demokratiska processen. Orsakerna är flera, men konsekvensen kan bli att det inte går att utöva de demokratiska rättigheterna fullt ut.

En viktig faktor för att kunna utöva det demokratiska uppdraget är att känna sig trygg och säker. Beroende på vilken nivå en politiker verkar har antingen Säkerhetspolisen eller Polismyndigheten ansvar för bedömningar av hot samt skyddsåtgärder. Men det är också viktigt att regelbundet lyfta säkerhetsfrågor och genomföra utbildningar både som enskild politiker och inom organisationen. Det finns även experter att ta hjälp av för att skapa trygga förhållanden. Säkerhet byggs tillsammans med andra i ett kontinuerligt utbyte och i återkommande dialog.

## Skydd av person

Säkerhetspolisen

**Säkerhetspolisen** har ansvar för bedömningar och skyddsåtgärder för den centrala statsledningen. Hit räknas statschefen, tronföljaren, talmannen, riksdagsledamöterna, statsministern, statsråden liksom statssekreterarna och kabinettssekreteraren. Det är Säkerhetspolisen som utreder brott mot den centrala statsledningen som har ett politiskt motiv och där våld, tvång eller hot förekommer.

Polisen

**Polismyndigheten** ansvarar för bedömning av hot och skyddsåtgärder för alla som inte faller under Säkerhetspolisens ansvar, såsom fritids-, kommun- och regionpolitiker, journalister och anställda inom exempelvis rättsväsendet.

**Egna bedömningar**

**Som enskild politiker** eller tjänsteman är det viktigt att även göra egna bedömningar och avvägningar. Här har också arbetsgivare ett arbetsmiljöansvar att säkerställa säkerheten för sina anställda. Oavsett vem som tar hand om skyddsåtgärderna så utformas de utifrån varje enskild situation där en noggrann bedömning av risken för hot och angrepp görs. Det kan till exempel röra sig om information och rådgivning, olika tekniska skyddsåtgärder, som att installera lås och larm, eller att använda sig av personbevakning, där den sista åtgärden är livvaktsskydd.

# Påverkansoperationer

Underrättelsehotet från andra länder mot Sverige har breddats och fördjupats. Det omfattar bland annat cyberattacker, spioneri och påverkansoperationer. Underrättelseverksamhet från andra länder pågår här och nu.

Vid sidan av den traditionella inhämtningen och spioneri genomför främmande makt en rad andra aktiviteter riktade mot Sverige. Dessa angrepp har breddats och fördjupats och riktas mot vårt ekonomiska välstånd, våra grundläggande fri- och rättigheter, vårt politiska självbestämmande samt vår territoriella suveränitet. Inte sällan sker påverkansoperationer genom försök att värva personer som har tillgång till information eller som ingår i ett nätverk av personer som är av intresse för främmande makt. Som politiker kan man därför bli mål för påverkansoperationer.

**Påverkansoperationer** kan exempelvis handla om försök att påverka beslut, uppfattningar eller beteenden hos den centrala statsledningen, befolkningen eller utvalda målgrupper. Som politiker är det här något som kan behöva hanteras. Det är därför av stor vikt att kontrollera den information som ges och vara källkritisk för att undvika att bli en del av en påverkansoperation. 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. Vid misstanke om påverkansoperation, kontakta säkerhetsansvarig samt Säkerhetspolisen.

# Personliga möten i syfte att värva

**Varje år utsätts** personer i Sverige för värvningsförsök. Genom underrättelseofficerare försöker främmande makt att rekrytera personer vars uppdrag är att samla information om Sverige och svenska förhållanden, en så kallad agent.

**Främmande makt** arbetar ofta långsiktigt. Politiskt aktiva kan bli uppsökta av exempelvis bekantskaper från tidigare i karriären. Mötet kan verka vara en tillfällighet, men om denna person efter en tids återupptagen kontakt i detalj börjar intressera sig för det politiska uppdraget och att få information bör det väcka misstanke. Det kan vara en del av så kallad kultivering, en fas i en långsiktig plan där främmande makts utsände söker vänskapsband med någon för att så småningom få denne att lämna ut upplysningar. Det yttersta målet kan vara att värva personen i fråga.

**Tänk på att alla** kan vara potentiella mål för ett värvningsförsök, det handlar om vem som kan ha eller skaffa sig access till önskad information. Det innebär även att personer i närhet till någon som har tillgång till säkerhetsklassad information kan utsättas för värvningsförsök. Vid misstanke om misstänkt kontakttagning eller ett värvningsförsök ska Säkerhetspolisen samt den egna säkerhetsorganisationen kontaktas.

**Om misstanke finns att värvningsförsök har gjorts**

- ☐ Anteckna vem som har gjort kontaktförsöket och vilken anledning personen uppgav till kontakten.
- ☐ Notera när och hur den första kontakten togs.
- ☐ Ta kontakt med Säkerhetspolisen samt med den egna säkerhetsorganisationen.

# Så värvas en agent

Varje år utsätts personer i Sverige för värvningsförsök, en process som kan delas upp i sex steg:

**Steg 1: Analys**
Analys av vilken information som den utländska underrättelsetjänsten behöver.

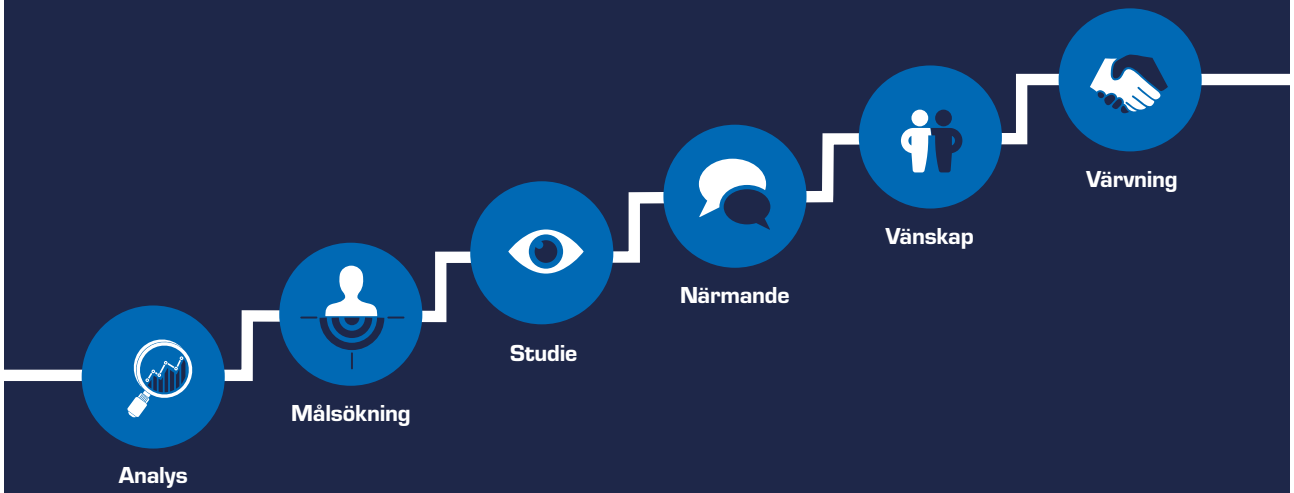
**Steg 2: Målsökning**
En underrättelseofficer får i uppdrag att hitta en person som kan dela med sig av den eftersökta informationen.

**Steg 3: Studie**
Personen som bedöms ha tillgång till rätt information kartläggs. Uppgifter om personliga egenskaper, svagheter, ekonomi och familjesituation ligger till grund för en bedömning av möjligheterna att få personen att arbeta för ett annat land.

**Steg 4: Närmande**
Underrättelseofficeren söker kontakt i en närmandefas. Närmandet ska uppfattas ske spontant eller slumpmässigt, även fast det i själva verket är mycket välplanerat.

**Steg 5: Vänskap**
Om första mötet blir lyckat inleder underrättelseofficeren en vänskapsrelation med den tilltänkta agenten. I den här fasen får den utvalda personen oskyldiga uppdrag för att testa relationen. Det kan handla om att bli ombedd att lämna över dokument som inte är hemliga. Personen vänjs också vid att ta emot gåvor av olika slag. Den här fasen kan pågå i flera års tid.

**Steg 6: Värvning**
Slutligen ställer underrättelseofficeren den tilltänkta agenten inför frågan att lämna ut hemlig eller känslig information. Om det faller väl ut har personen blivit agent för ett annat lands underrättelsetjänst.



# Kampanjarbete och offentliga möten

Under en valrörelse är en naturlig del i politikers vardag att träffa väljare genom att bland annat hålla offentliga möten, stå i en valstuga och knacka dörr. För att underlätta säkerhetsarbetet under en valrörelse behövs därför upparbetade rutiner och regelbundna riskanalyser.

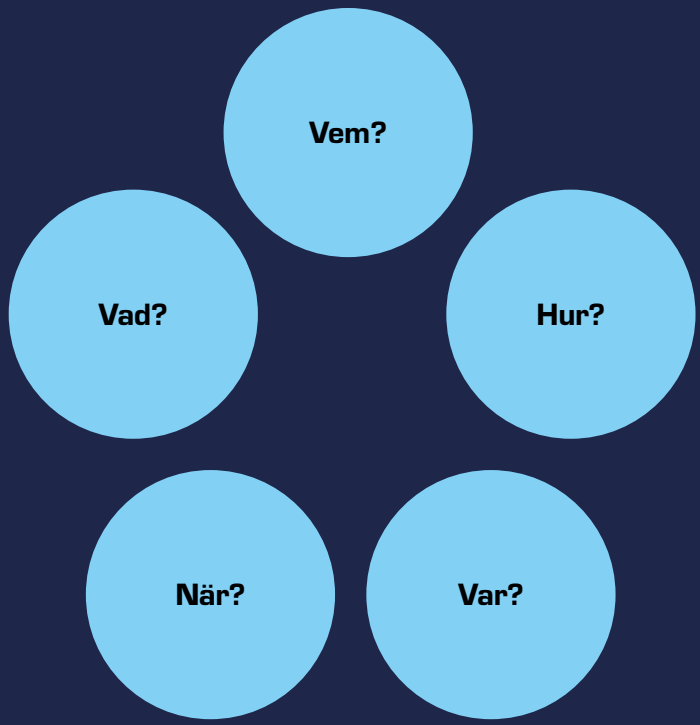
Ett första steg i säkerhetsarbetet är att göra en riskanalys, rådgöra med säkerhetsansvariga om de rutiner som finns, se över säkerheten och ha beredskap för störningar.

## Riskanalys

**I vår vardag** gör vi riskanalyser, mer eller mindre medvetet. En riskanalys är den process där risker identifieras och åtgärder som kan vidtas för att undvika eller minimera dessa risker bedöms. En riskanalys kan också vara mer detaljerad och omfatta särskilda aktiviteter eller säkerhetsåtgärder för en specifik situation. Ett exempel är de säkerhetsåtgärder som görs inför en lång resa, till exempel att hemmet larmas, anhöriga får adresser och resplaner samt var pass och resehandlingar placeras. En särskild riskanalys kan också göras för personer som är utsatta för hot.

**Ett politiskt engagemang** innebär ett behov av att regelbundet reflektera samt analysera risker och vilka sårbarheter som finns. Därför är det viktigt att försöka bedöma eventuella konsekvenser och reaktioner på exempelvis beslut som ska fattas eller uttalanden som ska göras. Ta gärna hjälp av organisationens säkerhets- eller kommunikationsavdelning för hjälp med detta. I sammanhanget är det viktigt att poängtera att varje arbetsgivare har ett arbetsmiljöansvar.

# Steg i en riskanalys




- Vilka aktiviteter behöver analyseras särskilt? Är det ett framträdande, ett känsligt beslut eller ett uttalande i en fråga som kan uppfattas som negativt eller kontroversiellt?
- Vem ska kontaktas för att få information eller för att rådgöra med?
- Vilka åtgärder kan vidtas för att minska risken eller konsekvensen?
- Var och när är det störst risk för att 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 på att hotfulla situationer kan ha sin upprinnelse i händelser som ligger långt tillbaka i tiden.

**Riskanalys vid offentligt möte**

- ☐ Bedöm 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 de frågor som ska lyftas under mötet varit hårt kritiserade bör det tas med i beräkningen.
- ☐ Ha en plan för hur de med ansvar för säkerheten ska agera vid oförutsedda händelser eller störningar.
- ☐ Bedöm behovet av resurser och bevakningsåtgärder som krävs för säkerheten. Samverka med Polismyndigheten eller Säkerhetspolisen, beroende på vem som har ansvar.
- ☐ Skaffa information om tillståndsfrågan gällande allmänna sammankomster via Polismyndigheten. I dialogen med Polismyndigheten bör de också informeras om eventuellt kontroversiella budskap.
- ☐ Ta reda på om Polismyndigheten känner till andra evenemang, till exempel om en demonstration ska hållas parallellt med det planerade mötet.
- ☐ Bedöm i god tid vilken information som ska gå ut inför mötet. Exempelvis vilka uppgifter kring mötet som kommuniceras i sociala medier. Var noggrann med vilka som informeras om detaljerna i programmet. Undvik att uppgifter som ankomsttid till hotell, när middag ska intas och liknande kommer ut till obehöriga.

# Möten med allmänheten

**När ett torgmöte** ska hållas, eller en scen eller ett talarpodium ska placeras, är det viktigt att huvudpersonen har ryggen fri. Det kan åstadkommas med hjälp av exempelvis en skyddad bakgrund eller fond.

**Undvik platser som** är på en yta där folk kan stå runt omkring. Vid placeringen är det även bra att tänka på angreppsrisken från personer och det eventuella kastavståndet fram till scenen. Säkerhetsavståndet till talaren kan skapas på olika sätt. Till exempel genom att sätta upp rep, band eller blommor. Det medför i regel även att folk ser bättre samt ger förvarning om någon försöker göra något. Tänk även på placeringen av entréer och av vakter eller funktionärer, samt var eventuella journalister kan stå. Om en mikrofon används för att publiken ska kunna ställa frågor är det viktigt att inte släppa den. Låt istället en medarbetare hålla mikrofonen åt den som vill ställa en fråga. Om någon kommer fram för att ge en gåva bör den helst packas upp av givaren själv.

# Ha beredskap för störningar

**För att tidigt** kunna hantera incidenter och spontana störningar som kan uppstå under ett evenemang är det viktigt att vidta förberedelser i god tid. Det kan handla om att förbereda åtgärder och rollfördelningar på plats, samt att upprätta bra kommunikationsvägar till de som ska bevaka arrangemanget. Om någon stör eller uppträder hotfullt under ett evenemang är det bäst att försöka undvika att provocera den personen. Ett tips är att lägga in nummer till viktiga kontakter såsom polis eller väktare i mobilen. Om ett akut läge skulle uppstå, ring nödnumret 112.

## Planera vägen ut

**Planera vägen ut** genom att lokalisera nödutgångar och ha en reträttväg klar till en säker plats om något skulle hända samt en säker parkeringsplats i nära anslutning till scenen. Undvik också att släppa in eller tillåta okända fordon att parkera i närområdet och rör er alltid tillsammans till och från evenemanget. Syftet är att snabbt kunna lämna en farlig situation och sätta sig i säkerhet tills situationen är under kontroll.

## Säkerhet vid dörrknackning

Som politiskt aktiv förekommer deltagande i olika slags kampanjer. Vid dörrknackning finns det flera delar att tänka på för att kunna genomföra det på ett så säkert sätt som möjligt.

**Säkerhet vid dörrknackning**

- ☐ Ha med mobiltelefon och bärbart larm om sådant innehas.
- ☐ Håll reda på var dörrknackningen tar plats om hjälp behöver tillkallas.
- ☐ Ha bil i närheten, om det är möjligt.
- ☐ Avbryt och lämna platsen om något känns hotfullt istället för att försöka ”rädda situationen”.
- ☐ Ta ett steg tillbaka efter att ha ringt på en dörr. Gå aldrig in till någon.
- ☐ Gå inte ensam! Ha andra kollegor eller partikamrater inom synhåll.

## Säkerhet vid bilfärder

**Bilen kan vara** en säker plats för att ta skydd i eller en möjlighet att hastigt lämna en farlig situation, men den kan också vara extra utsatt. Undvik därför att stiga ur bilen och ta direktkontakt vid en hotfull situation. Rådet är att istället försöka kommunicera genom bilrutan, kalla på hjälp eller ta sig till en plats där det finns andra människor. Ta även för vana att alltid ha låsta dörrar under bilfärden. Om misstanke finns att någon typ av kartläggning skett 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 bostadsadressen.

**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. Det är viktigt att alltid förvissa sig om att det fjärrstyrda centrallåset fungerar och att dörrarna verkligen går i lås. Det finns även speciella larm – så kallade paniklarm – som ger ifrån sig ett högt larmande ljud. Många bilar har även ett överfallslarm som aktiveras genom att trycka på en knapp på bilnyckeln.

**Taxi eller andra** taxiliknande tjänster ska helst förbeställas. Notera taxilegitimationen samt taxinumret vid taxiresa. Om möjlighet finns, betala i förväg med hjälp av en app då det gör att det går snabbare att ta sig ut ur bilen. Beställ taxi till en närliggande adress snarare än till hemadressen och samma sak på vägen hem. Be chauffören att stanna en liten bit från destinationen. Om taxiliknande tjänster som bokas via appar används, var noga med att kolla att registreringsnumret, bilmodellen och föraren stämmer med den information som finns i appen.

# Traditionella och sociala medier

Som politiskt aktiv är en del av jobbet att nå ut till sina målgrupper, bland annat genom medverkan i traditionella och sociala medier. Sociala medier bevakas även av massmedia och det finns ett stort intresse för politikers digitala närvaro.

Det är viktigt att alltid fundera i förväg kring vilka sammanhang och vilka platser som visas upp. Hemmet, familjen och miljöer som besöks regelbundet bör inte exponeras. Inte heller ska olika säkerhetsåtgärder som vidtas kommenteras. Uttalanden och kommentarer ska göras med eftertanke. Vid minsta tveksamhet är det att rekommendera att rådgöra med den egna organisationen innan publicering. Tänk även på att undvika att nämna arbets- eller partikamrater i intervjuer eller i kontakter med media om det inte är förankrat hos dem. Om pressansvariga finns på arbetsplatsen eller i partiet kan de rådgöras med vid osäkerhet. Hot ska alltid polisanmälas.

# Sociala medier

**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 man agerar och uttrycker sig. Sociala medier gynnar material som manar till engagemang, reaktioner och debatter, och är en viktig del av det demokratiska samtalet.

**Vägledning i sociala medier**

- ☐ Moderera kommentarer och ta fram en policy för hur hot- och hatfyllda kommentarer ska hanteras. Ta gärna hjälp av kommunikationsavdelningen eller annan del av organisationen med detta.
- ☐ Vid hot, skärmdumpa inläggen och användarprofilen samt ta kontakt med säkerhetsansvariga och Polismyndigheten eller Säkerhetspolisen. För hot gäller nolltolerans och hur de ska hanteras bör finnas formulerade i en policy.
- ☐ Var personlig men inte privat. Skapa en genomtänkt hållning för hur, när och vad som ska kommuniceras i sociala medier utifrån ett säkerhetsperspektiv.
- ☐ Överväg om det är lämpligt att i förväg, eller under ett pågående möte, berätta var det hålls. Använd inte incheckningsfunktioner som avslöjar den geografiska positionen om det inte är nödvändigt.
- ☐ Berätta helst om saker som redan har skett, och inte om saker som ska ske. Detta för att undvika kartläggning eller uppsökning av personer.
- ☐ Undvik att exponera eller ge en inblick i vanor som kan underlätta kartläggning, såsom tränings- eller shoppingrutiner eller platser som regelbundet besöks.
- ☐ Var noga med att alltid fråga om godkännande för publicering från de personer som medverkar i inlägg och på bilder.
- ☐ Var noga med att även i privata sammanhang berätta vad som gäller för egen medverkan i sociala medier. Be även vänner och familj att undvika angivelse av geografisk plats. Detta oavsett social medietjänst.
- ☐ Se över vad som exponeras på sociala medier. Exempelvis vilken sorts statusuppdateringar som görs i form av innehåll och foton. Publicera inte bilder så att det går att identifiera bostadsadressen.
- ☐ Se över säkerhetsinställningar med jämna mellanrum och aktivera tvåfaktorautentisering.
- ☐ Betrakta så kallade ”direktmeddelanden” på sociala medier som offentliga arenor. Allt som sägs där ska klara en granskning av såväl massmedia som av meningsmotståndare.
- ☐ Tänk på att säkerhets- och underrättelsetjänster runt om i världen systematiskt inhämtar information från öppna källor.
- ☐ Räkna med att den information som en gång lagts ut på internet alltid finns kvar.

**I digitala kanaler** kan det dock finnas situationer med individer vars enda syfte är att smutskasta eller förstöra samtalet. Vid sådana tillfällen är det viktigt att inte dras in i deras språkbruk. Kom också ihåg att det inte finns en skyldighet att fortsätta svara i digitala kanaler när debatten och språkbruket hamnat bortom rimliga gränser. Samtidigt sprids information fortare och till fler än någonsin förut. 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 eller vilseledande. Spridningen kan i sin tur leda till starka reaktioner och än starkare motreaktioner oavsett vem som publicerat informationen. 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 politiskt aktiva och deras organisation behöver ha en plan för hur de ska agera. Hotbilden kan höjas på kort tid och det kan uppstå behov av att snabbt analysera, nyansera eller dementera uppgifter som cirkulerar. En utarbetad plan kan också vara ett bra stöd vid beslut om eventuella säkerhetsåtgärder om situationen skulle bli allvarlig. Använd blockeringsfunktioner på tjänster vid behov.

**Tänk även på** den personliga integriteten i sociala medier. Använd helst en stängd profil, det vill säga att profilen endast är synlig för personer som godkänts. Ett råd är att skapa en öppen offentlig sida i sociala medier som hålls avskild från ens privata sida. Var också noga med att ofta byta lösenord och ha en avancerad inloggning till kontona.

# Källkritik

**I dagens medielandskap** nås vi av information från många olika källor, och det är inte alltid lätt att se och veta vad som är verkligt eller inte. Därför är det viktigt att vara källkritisk. Ett kritiskt tänkande garanterar inte att man undviker att bli lurad, men det gör medvetenheten om riskerna större.

**Några källkritiska kontrollfrågor**

- ☐ Vem är avsändaren?
- ☐ Vad är det bakomliggande syftet med informationen? Är det propaganda eller information?
- ☐ Hänvisas det till källor?
- ☐ Finns det fler källor som säger samma sak?

Tips: På Internetstiftelsens webbplats www.internetkunskap.se finns mer information om källkritik.

# Hantera hot och angrepp

Att vara förberedd på hot kan göra det lättare att agera korrekt. Det kan handla om att i förväg tänka på olika scenarier och se olika handlingsalternativ framför sig. Detta oavsett om situationen skulle uppstå i samband med ett offentligt framträdande, på nätet, på arbetsplatsen eller i anslutning till bostaden.

En direkt reaktion på ett hotfullt meddelande kan vara att snabbt radera det. Men för att någon ska kunna lagföras är det viktigt att inte radera hot eller trakasserier som kommer in via e-post, sociala medier eller sms. De behövs i digital form bland annat för att kunna spåra var de har skickats från. Vissa meddelanden raderas med automatik efter en viss tid eller om avsändaren väljer att ta bort meddelandet, beroende på plattform. Därför är det viktigt att ta en skärmdump.

**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. Genom att vara uppmärksam på vad som händer kan sättet att agera anpassas utifrån situationen och hur den förändras. Försök att vara saklig även vid provokationer. Vid samtal med en person, försök få denne att bryta sitt handlingsmönster genom att föreslå alternativ till dennes agerande.

**Om en situation är hotfull** gäller det att både bedöma avsikten hos personen ifråga samt vilken typ av agerande som krävs. Det kan handla om att ropa på hjälp, fly från platsen eller att försvara sig. Handla alltid med eftertänksamhet och försök att agera med initiativ och handlingskraft.

## Vad är ett hot?

**Dessvärre händer** det att politiker får ta emot både hot och hat. Hat är obehagligt att motta, men att skriva hatiska kommentarer till någon behöver i sig inte vara brottsligt. Hot behöver inte heller alltid vara det, utan det beror på hur det är utformat. Om antalet hatfulla kommentarer eller liknande ökar bör säkerhetsansvariga kontaktas då det kan vara en indikation på en ökad hotbild. Ibland kan det dock vara svårt att skilja mellan de två. Vid osäkerhet om det är ett olaga hot eller inte, prata med den egna säkerhetsorganisationen och bedöm om agerandet ska polisanmälas.

§ **Exempel på brott:**

**Olaga hot 4 kap. 5 § brottsbalken**
Hot om brottslig gärning på sätt som är ägnat att hos den hotade framkalla allvarlig rädsla för egen eller annans säkerhet till person, egendom, frihet eller frid. Hot om brottslig gärning kan vara något som uppfattas som ett påstående om att ett brott kommer att utföras. Hotet kan till exempel avse våld mot person eller skadegörelse. Även förtäckta hot kan utgöra sådant hot, om brottslig gärning antyds på något sätt.

**Ofredande 4 kap. 7 § brottsbalken**
Brottet ofredande är när någon fysiskt antastar eller utsätter någon annan för störande kontakter eller annat hänsynslöst agerande om det är ägnat att kränka den utsattes frid på ett kännbart sätt. Med störande kontakter avses kontakter såväl vid personliga sammanträffanden som elektronisk kommunikation.

**Olaga förföljelse 4 kap. 4b § brottsbalken**
Brottet olaga förföljelse kan vara aktuellt när det sker upprepade kränkningar mot en och samma person, till exempel olaga hot och ofredande, och var och en av gärningarna har utgjort ett led i en upprepad kränkning av den personens integritet.

# Anmäl alla hot

**Om hot, våld** eller trakasserier förekommer trots förebyggande åtgärder finns det flera saker att göra. Hot som upplevs som allvarligt och brottsligt ska polisanmälas. Informera också internt säkerhetsansvariga på arbetsplatsen eller närmaste chef om det inträffade. Dokumentera och spara även sådant som har anknytning till brottet då det kan underlätta utredningen.

**Beroende på vem** hotet är riktat mot och motivet bakom hotet är det antingen Säkerhetspolisen eller Polismyndigheten som utreder brottet. Säkerhetspolisen är ansvarig för den centrala statsledningen. Om exempelvis ett hot framförs mot någon i den centrala statsledningen och hotet är politiskt motiverat samt handlar om olaga hot eller olaga förföljelse är det i grunden Säkerhetspolisens ansvar.

**I och med** en anmälan kan brottsoffer- och personsäkerhetsarbetet inledas. En anmälan underlättar också underrättelsearbetet. Även i de fall där en anmälan inte kan knytas till en gärningsperson, så kan den vara en viktig pusselbit för att analysera liknande brott och tillvägagångssätt. I samband med polisanmälan kan polisen ge information om lämpligt brottsofferstöd och vad som kan göras för att skydda sig själv och sina närmaste. Om en hotbild finns görs en skyddsplan och eventuella säkerhetsåtgärder planeras i dialog med den utsatta. Det är Säkerhetspolisen alternativt Polismyndigheten samt 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 skyddsarbetet och kan leda till att en gärningsperson identifieras, åtalas och döms. I andra fall saknas möjlighet att driva utredningen framåt och förundersökningen läggs ned, men då kan skyddsarbetet ändå fortsätta. Det är med andra ord inte avhängigt om en gärningsperson identifierats eller inte, utan skyddsarbetet utformas efter det behov som finns.

## Nödvärn

**Var och en** har rätt att försvara sig själv och sin egendom utan att det är brottsligt så länge som det 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.

**§ Bestämmelsen om nödvärn**
finns i 24 kap. 1 § brottsbalken.

## Hot på telefon och internet

**Hot eller trakasserier** via telefon eller via internet bör snarast anmälas till Säkerhetspolisen alternativt till Polismyndigheten beroende på vem som fått motta hotet. Även den egna säkerhetsorganisationen bör informeras. I en eventuell brottsutredning kan det finnas möjlighet att spåra vem som använt det aktuella telefonnumret eller IP-adressen. Lyssna uppmärksamt och avbryt inte den som ringer. Notera tid, bakgrundsljud, kön, ålder, dialekt och liknande. Om möjligt spela in samtalet. Genom att upprepa det som den uppringande säger och låtsas som att det inte går att höra ordentligt samt genom att använda fraser som ”Förlåt, jag hörde inte riktigt vad du sa?” förlängs samtalet vilket kan ge mer information och därmed underlätta identifieringen av den uppringande. Tänk på att inte radera hot som kommit in via e-post, sociala medier eller sms då de behövs i digital form för att kunna spåra var de har skickats ifrån. Gör skärmdumpar på det som går.

# Säkerhet i vardagen

En del i att kunna känna sig trygg och säker i sin bostad och vardag är att ha säkerhetsåtgärder på plats både i hemmet, för familjen och på arbetsplatsen.

Känslan att vara trygg och säker i sin bostad kan öka genom att ha ett skalskydd och därmed säkra de vanligaste intrångsvägarna: entrédörrar, fönster som lätt kan nås, stegar som kan användas för att ta sig förbi skalskyddet samt takluckor. Ett annat råd är att be grannar att hålla ett öga på bostaden när ingen är hemma.

**De som lever** under hot bör planera för alternativa utrymningsvägar i hemmet. Beroende på hur hotsituationen ser ut kan säkerhetspersonal eller annan kvalificerad personal, och i särskilda fall Säkerhetspolisen eller Polismyndigheten, bistå med säkerhetsrådgivning. Rådgivningen kan belysa specifikt hur skyddet i bostaden eller på arbetsplatsen kan förbättras eller beröra säkerhetsaspekter i närmiljön.

## Dörrar och brevinkast

**För boende** i lägenhet är en säkerhetsdörr med extern förstärkt brevlåda det bästa skyddet. Om ytterdörren har ett brevinkast kan en förebyggande åtgärd vara att montera en säkerhetsbrevlåda med brandskydd på insidan av dörren. Istället för brevinkast kan en utvändigt låsbar brevlåda eller en postbox användas.

**Dörrar och brevinkast**

- ☐ Dörrarna till bostaden bör ha en skyddsnivå som motsvarar inbrottsskyddade dörrar enligt gällande standard.
- ☐ Dörr- och fönsterkarmar ska ha samma skyddsnivå som dörrar och fönster.
- ☐ Se till att fönster samt balkong- och terrassdörrar som kan nås från markplanet har samma skyddsnivå som entrédörrarna.
- ☐ Montera en dörrkik på entrédörren. Via vidvinkelfunktion kan faror upptäckas och personer identifieras utan att öppna dörren. Undvik insyn med ett skydd över dörrkiken på insidan av dörren.
- ☐ Ha god belysning utanför dörrar, vid uppfarten samt i trädgården om en sådan finns.

## Fönster och glasade ytor

**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 en speciell plastfolie monteras på insidan av glaset som ger ett visst inkasts- och insynsskydd. Sidoljus som är integrerade i dörrpartiet bör ha samma skyddsnivå som dörren.

## Nycklar, kort och koder

**Nycklar, inpasseringskort** och portkoder kan utnyttjas för att komma förbi skalskyddet. Skydda dessa så att de inte kommer i orätta händer. Om nycklar, inpasseringskort eller koder tappas bort är det viktigt att omedelbart meddela hyresvärden eller bostadsrättsföreningen. 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 med hjälp av kemikalier som är avsedda för detta ändamål. Byt därför kod och rengör knappsatsen regelbundet. Nycklar och lås ska även vara godkända enligt gällande standard där nycklarna ska vara kopieringsskyddade, helst med behörighetskort. Elektroniska ytterlås ska vara godkända av försäkringsbolaget samt certifierade.

**Nycklar, kort och koder**

- ☐ Håll bostadsnycklar åtskilda från andra nycklar.
- ☐ Se till att nycklar, kort och koder inte kan identifieras.
- ☐ Byt låscylindrar om nycklar kommit på avvägar.
- ☐ Förvara inte nycklar på platser som lätt kan upptäckas eller där en personlig sammankoppling kan göras.
- ☐ Lämna aldrig nycklar till någon som inte är betrodd. Tänk på risken att nycklarna kopieras.
- ☐ Byt lås vid flytt till ny bostad.

# Familj – skyddet för närstående

**En förövare kan** pröva att gå via närstående för att försöka påverka förmågan att fungera i det politiska uppdraget. 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.

# Larm och säkerhetsåtgärder

**Det finns en** rad olika larm – fasta och mobila – för att skydda både bostad och person. Anpassa larmet utifrån boendemiljön för att minimera risken för onödiga larm och därmed även oönskade insatser från bevakningsbolag eller polis. Det kan handla om att se över olika utrymmen som kan behöva larmas, om det finns husdjur i hushållet eller vilken typ av larmsystem som fungerar bäst. Det är även viktigt att fundera på vilka säkerhetsåtgärder som ska vidtas om larmet går, oavsett om det sker på dagen eller natten. Larmmottagning bör ske till en dygnet-runt-bemannad och godkänd larmcentral. Var försiktig med att använda fjärrkontroller och appar för att styra ett larm. Risken finns att någon obehörig kan ta över.

**Ett inbrottslarm** är en extra säkerhetsåtgärd. I hus bör entré- och balkongdörrar, glasade partier och garage skyddas av larmet. Det kan vara ett ljudande larm, en siren eller ett tyst larm som överförs till en larmcentral. Många larm har även en kamera kopplad till sig för

**Familj – skyddet för närstående**

- ☐ 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.
- ☐ Var uppmärksam på okända personer som rör sig oförklarligt i närområdet eller söker kontakt på arbetsplatsen, i skolan eller under en fritidsaktivitet.
- ☐ Var försiktig med gåvor från okända.
- ☐ Kontrollera besökare till bostaden genom dörrkik eller fönster.
- ☐ Släpp inte in okända personer i bostaden eller trappuppgången.

**Om det finns en hotbild bör exempelvis personal vid förskola och skola samt ledare inom fritidsaktiviteter informeras. Den som hämtar barnen ska heller inte vara okänd för personalen.**

- ☐ Instruera barnen i hur och när de ska larma nödnumret 112.
- ☐ Be barnen att gå tillsammans med en kamrat eller vuxen till och från skolan och olika fritidsaktiviteter.
- ☐ Meddela alla förändrade tider, till exempel rörande hämtning från skolan och fritids-aktiviteter.

att verifiera eventuella obehöriga. Idag kan de flesta övervakade larm dessutom kompletteras med rökdetektorer vilket skapar en högre skyddsnivå vid bränder. Ett råd är att sätta upp en skylt om bevakning eller larm vilket kan vara avskräckande.

**För den som** är, eller riskerar att bli, utsatt för hot, våld eller trakasserier kan det vara motiverat att ha ett överfallslarm eller personlarm. Olika former av bärbara överfallslarm tillhandahålls av larmoperatörer, bevakningsbolag och andra branschföretag. Personlarm används via en mobiltelefon genom att position och nödsignal sänds till en förprogrammerad mottagare med en enkel knapptryckning.

## SOS Alarm

**I nödsituationer** går det normalt sett att larma till 112 även om telefonnätet eller SIM-kortet inte fungerar. Om 112 kontaktas utan SIM-kort eller är roamad till ett nät som den normalt inte har tillgång till visas inte telefonnumret för SOS Alarm.

**SOS Alarm har** även en app där positionen skickas per automatik vilket underlättar att snabbt få hjälp på plats. Rekommendationen är att använda den för att ringa upp 112 för positionering av mobiltelefonen. Via appen går det även att dela sin egen position med valfri person. SOS Alarm får i de flesta fall även hjälpsökandes position via mobilens GPS eller utifrån omgivande mobilnät via funktionen AML (Advanced Mobile Location) som finns i telefonens operativsystem.

## ICE visar anhörigas telefonnummer

**Genom att lägga** in en post under kontakter i mobiltelefonens adressbok och kalla den ICE (In Case of Emergency) kan räddnings- och sjukvårdspersonal komma i kontakt med anhöriga eller andra kontakter i händelse av sjukdom eller olycksfall. Posten ICE används internationellt och kan innehålla telefonnummer till ett valfritt antal personer. I många mobiltelefoner finns olika förinstallerade funktioner eller appar som gör att det går att se ICE-kontakterna även om telefonen är låst.

## Säkerhet på 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 arbetsplatsen eller partilokalen. 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. Det är även viktigt att se över säkerheten i hemmet i de fall det används som arbetsplats.

## Säkerhet på arbetsplatsen och i hemmet

**På arbetsplatsen:**

- ☐ Fråga säkerhetsansvariga eller närmaste chef om aktuella säkerhetsåtgärder och vilka säkerhetsrutiner som gäller. Om brister upptäcks ska detta påpekas så de kan åtgärdas.
- ☐ Se till att det finns en rutin kring hur oanmälda besökare hanteras.
- ☐ Informera berörda medarbetare samt säkerhetsansvariga eller partiorganisationen 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 obehagliga situationer ska bemötas.
- ☐ Undvik att ta emot okända besökare i enrum. Om misstanke finns att mötet kan bli obehagligt eller situationen känns osäker, be någon att sitta med på mötet. Säkerställ att det är enkelt att lämna rummet och larma vid hot eller angrepp.
- ☐ Eskortera besökarna i lokalerna och lämna inte obehöriga utan uppsikt.
- ☐ Var uppmärksam på kvarglömda väskor och annat som kan innehålla farliga föremål.
- ☐ Undvik rutiner och variera färdväg och restider om det finns risk för angrepp.

**När hemmet används som arbetsplats:**

- ☐ Använd inte arbetsutrustningen för privat bruk och låna inte ut den till andra.
- ☐ Logga alltid ut så ingen annan kan få åtkomst till information när datorn eller annat uppkopplat arbetsverktyg inte används.
- ☐ Använd endast USB-minnen som är godkända för användning i arbetsdatorn. USB-minnen som är privata ska inte användas i en arbetsdator och vice versa.
- ☐ Skydda viktig information som finns på papper och i anteckningar.
- ☐ Vid digitala arbetsmöten, bedöm både om mötet är lämpligt att genomföra digitalt, samt risken för att andra kan höra eller se det som diskuteras.
- ☐ Se över vad som visas vid skärmdelning. För att undvika att andra kan se annat än det som avses att delas, stäng ner program och dokument som inte ska visas och dela inte hela skrivbordet.
- ☐ Om kameran är på vid digitala möten, sudda ut bakgrunden om möjligt eller visa en annan bakgrund och undvik att visa bilder på familjemedlemmar och andra personliga saker.
- ☐ Om andra kan se din skärm, använd ett godkänt skärmskydd på datorn.
- ☐ Arbeta inte i samma rum som andra enheter som är anslutna till nätverk.
- ☐ Resonera med den egna organisationen och säkerhetsorganisationen kring cybersäkerhet och ta reda på vilka regler som gäller för uppkoppling mot arbetsplatsen och för hemarbete.

Läs mer under kapitlet Säker hantering av teknisk utrustning.

Tips! Mer information om säkrare arbete utanför arbetsplatsen finns att läsa på Myndigheten för samhällsskydd och beredskap, www.msb.se.

# Säker hantering av teknisk utrustning

Oftast kan det politiska uppdraget utföras som det är tänkt, men säkerhetshotet från de som vill skada Sverige och demokratin har ökat. Den tekniska utrustning som vi använder i allt större utsträckning gör oss också mer sårbara. För att minska risken att utsättas är det viktigt att ha en säker hantering av den tekniska utrustningen.

Trådlösa nätverk (WiFi) öppnar upp för andra att lyssna av och göra intrång. Samtidigt har det blivit allt lättare att spåra personer med hjälp av appar och geopositionering. 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 är det viktigt att ha en säker hantering av den tekniska utrustningen i form av bland annat mobiltelefoner, datorer och andra uppkopplade enheter. Risken finns att informationen kan användas i brottsliga syften, exempelvis för bedrägerier, hot, trakasserier eller angrepp. Tänk på att känslig information som inte skyddas kan överhöras eller hamna hos obehöriga genom slarv eller okunskap. Det är även viktigt att se över vad enheterna, som exempelvis hörlurar, är döpta till då det kan bli lätt att identifiera vem som är i ett visst område eller utrymme.

# Trådlösa nätverk

**Mobiltelefoner,** surfplattor, aktivitetsarmband, smarta klockor och andra uppkopplade enheter är idag något de flesta använder. Uppkopplingar som sker från dessa är oftast säkra. 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 kan det medföra att en obehörig får tillgång till privata uppgifter, det vill säga får en fullständig bild av till exempel personliga kontakter, kalender och rörelsemönster samt kan läsa e-post. Ett sådant intrång kan också innebära att funktioner i enheten används i den utsattes namn, exempelvis att det skickas e-post eller läggs ut inlägg på sociala medier av någon annan än den som står bakom kontot.

**För att öka** säkerheten kan telefonen och dess innehåll förses med särskild kryptering, men tänk på att appar som krypterar meddelanden som exempelvis Signal, Telegram eller WhatsApp inte ska användas för att skicka säkerhetsskyddsklassade uppgifter. Mobiltelefoner kan lokaliseras med hjälp av telefonnumret. Observera att mobiltelefonen kan lokaliseras även om numret är hemligt eller har ett så kallat kontantkortsnummer. En mobiltelefon och andra uppkopplade enheter kan även lokaliseras med hjälp av trådlösa uppkopplingar. Om WiFi är påslaget på telefonen söker den aktivt efter nätverk för åtkomst till internet och vid dessa tillfällen annonserar telefonen sig själv. Därför bör aldrig andra WiFi-nät än arbetsplatsens användas. Då är det säkrare att använda uppkoppling via mobilnätet. Var medveten om att all information som skickas eller tas emot via trådlösa nätverk kan läsas av andra om anslutningen inte är säker.

### Användning av WiFi

- ☐ Använd inte WiFi om det inte är absolut nödvändigt. Använd istället mobilens nät eller ett modem kopplat till mobilnätet. Om WiFi har använts, stäng av efter användning.
- ☐ Om trådlösa nätverk används, 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, och att inte använda en föråldrad krypteringsfunktion.
- ☐ Anslut aldrig till öppna trådlösa nätverk, eftersom datatrafiken då kan övervakas av vem som helst som är på nätverket.
- ☐ Om anslutning till ett öppet WiFi måste ske bör det kombineras med så kallad vpn-anslutning.

# Datorer och teknisk utrustning

**Undvik att använda** offentliga datorer eller anslutningar när information hanteras som inte ska hamna i orätta händer. Vid användning av någon annans utrustning, till exempel på hotell, bibliotek eller internetkafé, utgå från att någon kan komma över inloggningsuppgifter eller annan känslig information. Tänk på att ta bort temporära internetfiler från webbläsaren efter användandet. För att vara extra försiktig är ett råd att byta lösenord på det e-postkonto som använts på den allmänna datorn. Observera att detta bara är en begränsad åtgärd. Det går aldrig att veta hur mycket av aktiviteterna som sparats på en dator som någon annan äger. Utgå från att allt sparas. E-post ska läsas på ett skyddat sätt genom säker inloggning och en krypterad förbindelse, det vill säga en vpn-tunnel.

**Datorer och teknisk utrustning**

- ☐ Undvik att lämna och förvara teknisk utrustning utan uppsikt, till exempel i bilar, på hotellrum eller på restauranger.
- ☐ Var rädd om inloggningsuppgifter till datorer så att ingen obehörig kommer åt dem.
- ☐ Notera koder och nummer för att kunna spärra abonnemang om något skulle ske.
- ☐ Stoppa aldrig in okända USB-enheter eller minneskort i datorn.
- ☐ Installera, aktivera och uppdatera kontinuerligt antivirusprogram och personliga brandväggar.
- ☐ Uppdatera också operativsystemet och gör säkerhetsuppdateringar regelbundet. Äldre versioner får inte alltid nya säkerhetsuppdateringar. Därför är det viktigt att byta ut enheten om säkerhetsuppdateringar upphör från leverantören.
- ☐ Använd aldrig samma lösenord i privata sammanhang som 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 jobbets e-postadress i privata sammanhang eller för att skapa konton på andra sajter än sådana som är relevanta för arbetet.
- ☐ Nätfiske, eller phishing som det också kallas, förekommer både bland kriminella och främmande makt. Klicka aldrig på länkar i e-posten och öppna heller aldrig filer från okända avsändare. Ange aldrig personliga koder efter uppmaning via sms eller e-post. Inga seriösa aktörer skickar sådana uppmaningar. Logga heller inte in med bank-id eller liknande. På Polismyndighetens hemsida finns mer information om skydd mot nätfiske att läsa.
- ☐ Nyttja inbyggda funktioner i enheten för att kryptera hårddiskar och annat lagringsmedia.

# Säker hantering av mobiltelefoner, appar och uppkopplade enheter

**Mobiltelefoner** och många av dess funktioner och appar gör vårt liv lättare, men genom geopositionering i bland annat mobilen och aktivitetsband blir det samtidigt lättare att spåra och kartlägga exempelvis träningsrutiner, rörelsemönster, kontakter, var barnen går i skolan, intressen och var någon bor. I samband med att vissa appar installeras ges de även tillgång till gps-positionering. Information som sedan kan

**Säkrare hantering av mobiltelefonen**

- ☐ Glöm inte att regelbundet uppdatera programvaran och apparna i mobiltelefonen.
- ☐ Använd kodlås (pinkod), FaceID eller fingeravtryck och telefonlås på mobiltelefonen.
- ☐ Håll telefonen under uppsikt. Lämna den inte till någon obehörig då det finns risk för manipulation.
- ☐ Ha inga mobiltelefoner eller andra uppkopplade enheter i sammanhang eller rum där särskilt förtroliga eller hemliga samtal förs.
- ☐ I många mobila enheter finns standardinställningar som tillåter trådlös överföring av data. Ta därför för vana att alltid stänga av trådlös överföring av data som inte används, till exempel Bluetooth (blåtand), AirDrop eller närfältskommunikation (Near Field Communication, NFC).
- ☐ Acceptera inga oväntade programinstallationer via e-post, sociala medier, sms eller liknande.
- ☐ Använd inga okända minneskort i telefonen.
- ☐ Om mobilen innehåller känslig information överväg att frångå externa leverantörers erbjudande av säkerhetskopiering av innehållet.
- ☐ Kopiera över all information innan mobiltelefonen lämnas in för service eller uppgradering, samt gör en så kallad total återställning eller Master Reset.
- ☐ Kolla med organisationens it- eller säkerhetsansvariga vad de rekommenderar för inställningar i mobiltelefonen.

**Appar i mobilen:**

- ☐ Uppdatera appar och operativsystem, men tänk på att se över integritetsinställningar efter en uppdatering då de kan ha ändrats.
- ☐ Läs användarvillkoren noga innan installation av en ny app. Ge appen ett minimum av behörigheter för att den ska fungera.
- ☐ Logga ut från appar när de inte används, annars kan de arbeta i bakgrunden.
- ☐ Radera appar som inte används. Glöm inte att radera tillhörande konto också.
- ☐ Gå igenom och reglera behörigheterna i apparna regelbundet.
- ☐ Var restriktiv med att ge appar tillgång till positionsdata. Slå bara på om det behövs.

hamna i databaser som säljs vidare. Även om den är anonym kan den lätt avanonymiseras. Kom ihåg att även ett träningsarmband, en smart klocka eller uppkopplade bilar kan avslöja gps-positionen.

**Det finns också** appar som automatiskt kontrollerar var mobiltelefoner befinner sig och inkluderar positionen i exempelvis foton, sökningar, webbsidor och uppdateringar på sociala medier. Om geopositioneringen är påslagen på bilder följer taggningen med bilderna även i samband med att de delas. Se därför över om det är en funktion som är nödvändig eller om den kanske ska slås av. Ta hjälp av säkerhetsorganisationen för att ha rätt inställningar.

Tips! Mer information om integritet i mobilen finns att läsa på Internetstiftelsens webbplats www.internetkunskap.se.

## Risk för avlyssning trots kryptering

**Sekretessbelagd information** ska aldrig avhandlas via mobiltelefon eller bärbara enheter om de inte har signalskyddssystem 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. Förutom att lämna mobiltelefoner utanför rummet när sekretessbelagd information avhandlas, tänk på att även andra uppkopplade enheter såsom aktivitetsband, smarta klockor och hörlurar kan avlyssnas och inte ska finnas med i rummet.

Tips! På www.informationssakerhet.se finns fördjupande fakta om arbetet med att säkra kryptografiska funktioner.

# Skydda den personliga integriteten och identiteten

I takt med att det blir allt lättare att exempelvis ta reda på personuppgifter och var någon bor kan det vara bra att veta vad som går att göra för att skydda sig. Det kan vara allt från att minska synlig- och spårbarheten på nätet till att skydda personuppgifterna eller få ett kontaktförbud utfärdat.

Ibland är hotbilden sådan att det inte räcker med att vidta normala försiktighetsåtgärder, utan det krävs att andra säkerhetsåtgärder kopplas på för att skydda den personliga integriteten och identiteten.

## Kontaktförbud

**Syftet med kontaktförbudet** är att förebygga brott, förföljelse eller andra allvarliga trakasserier. Att överträda ett kontaktförbud är brottsligt och kan leda till böter eller fängelse upp till två år. Kontaktförbudet är tidsbegränsat. Begäran om kontaktförbud kan göras muntligen eller skriftligen till Åklagarmyndigheten eller Polismyndigheten som också kan svara på frågor. En åklagare eller en domstol beslutar om kontaktförbud.

Det finns fyra olika grader av kontaktförbud:

- **Ordinärt kontaktförbud,** innebär att personen förbudet avser inte får besöka, kontakta eller följa efter den skyddade personen.
- **Kontaktförbud i gemensam bostad,** innebär att förbudspersonen inte får vistas i en bostad som brukas gemensamt med skyddspersonen.
- **Utvidgat kontaktförbud,** innebär att den person förbudet gäller, inte får besöka eller vara i närheten av den skyddade personens bostad, arbetsplats eller andra ställen där hon eller han brukar vara. Om ett kontaktförbud som tidigare utfärdats överträtts ska det utvidgade kontaktförbudet förenas med beslut om elektronisk övervakning.
- **Särskilt utvidgat kontaktförbud,** innebär att den person 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. 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.

# Skyddade personuppgifter

Uppgifter som registreras i folkbokföringen är som huvudregel offentliga. En eventuell gärningsperson kan alltså med hjälp av uppgifter från folkbokföringen ta reda på uppgifter som i förlängningen möjliggör 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. Det finns tre olika typer av skyddade personuppgifter:

- **Sekretessmarkering**
  Den vanligaste formen av skyddade personuppgifter är sekretessmarkering, vilket är den lägre graden.
- **Skyddad folkbokföring**
  Genom en skyddad folkbokföring är den faktiska bostadsadressen inte registrerad via folkbokföringsdatabasen. Ansökan görs till Skatteverket.
- **Fingerade personuppgifter**
  En helt ny identitet skapas. Detta används som en sista utväg för personer som är utsatta för särskilt allvarlig brottslighet som riskerar liv, hälsa och den personliga friheten. Fingerade personuppgifter hanteras av Polismyndigheten.

# Sekretessmarkering i vardagen

**Sekretessmarkering** gör det svårare att ta del av de personuppgifter som finns i folkbokföringsdatabasen. En sekretessmarkering kan Skatteverket registrera om det finns anledning att anta att en person eller närstående till denne kan komma att lida skada om deras uppgifter lämnas ut. Ansökan om sekretessmarkering görs till Skatteverket. I samband med ansökan ska hotbilden styrkas, till exempel genom att bifoga en kopia på polisanmälan. Om den enskilde beviljas sekretessmarkering registrerar Skatteverket denna i folkbokföringsdatabasen. Markeringen meddelas andra myndigheter och fungerar som en varningssignal till dem. 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 görs, var medveten om att det även komplicerar familjens vardag. Det kan handla om praktiska saker som att barnen inte kan vara med på skolfoton eller klasslistor, eller att det kan bli svårt att teckna avtal vid köp av varor eftersom uppgifterna inte syns i de offentliga registren som butiken har tillgång till. Även köp över internet och användning av bank-id kan försvåras. Rekommendationen är att sekretessmarkeringen bör omfatta samtliga familjemedlemmar som bor på samma adress så det inte går att spåra via dem. Även om en sekretessmarkering försvårar kartläggning och spårning, kan den inte helt garantera säkerheten. Tänk på att bank, post, skola, läkare, föreningar och andra organisationer inte per automatik får uppgift om sekretessmarkeringen. Därför kan de behöva kontaktas för att skydda uppgifterna.

# Id-kapning

**Med id-kapning** eller identitetsintrång menas vanligtvis att någon köper varor eller tar krediter i någon annans namn. Ett annat syfte kan vara att använda identiteten på sociala medier för att exempelvis sprida falska påståenden. Ha kontroll på id-handlingar, var vaksam om någon gör en kreditupplysning och polisanmäl direkt vid misstanke om brott. Id-stöldskydd ingår även i många hemförsäkringar.

# Upplysningstjänster

**I Sverige får** alla utgivare med utgivningsbevis dela med sig av information som finns i folkbokföringen. I korthet innebär det att en webbplats med ett utgivningsbevis har ett grundlagsskydd enligt yttrandefrihetslagen. Därför har webbplatser där uppgifter om exempelvis adress, telefonnummer, födelsedag eller brottsregister ett lika starkt skydd som nyhetssajter. Det här gör att det kan vara svårt att bli helt borttagen från vissa webbplatser med utgivningsbevis. En del går med på att ta bort uppgifterna, medan andra inte gör det. Från en del går det även att bli raderad från det publika söket, men uppgifterna är då fortfarande synliga i inloggat läge. Det är upp till varje utgivare att gå med på att radera en persons uppgifter.

**I dagsläget är** det enda sättet att helt bli bortplockad från upplysningstjänster att kontakta Skatteverket och ansöka om skyddade personuppgifter, men det beviljas enbart vid utsatthet för ett allvarligt och konkret hot. Det går även att kontakta sin telefonoperatör och ange att ens telefonnummer ska vara dolt för nummerupplysningstjänster. Då kommer numret inte att visas på deras sidor, men de andra uppgifterna kommer även fortsättningsvis att visas.

Tips! Mer information om detta går att läsa hos Integritetsskyddsmyndigheten, www.imy.se.


3440 4-
34507
34508-
34609

# Avvikande och icke beställda försändelser

Post som skickas hem eller till arbetsplatsen kan innehålla obehagliga överraskningar och är samtidigt något som är svårt att skydda sig emot. En adress är ofta enkel att få tag på och att skicka paket eller brev med oönskat innehåll till någon är ett lätt tillvägagångssätt för en gärningsman.

Det är därför viktigt att vara uppmärksam på icke beställda och avvikande försändelser och att be familjen att agera på samma sätt. Om barn finns i familjen bör de helst inte öppna post eller paket. Farliga försändelser ska alltid polisanmälas. Även ofarliga försändelser kan upplevas som hotfulla, som trakasseri eller som otillbörlig påverkan. Även detta bör polisanmälas. Ett sätt att minska risken att utsättas för försändelser till hemadressen är att posten skickas till arbetsgivaren istället för till hemadressen. Ett annat sätt är att få en sekretessmarkering hos Skatteverket. Läs mer om det på sidan 38-39.

# Avvikande försändelser – några kontrollfrågor

**Avvikande försändelser**

- ☐ 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 handskrift.
- ☐ 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 arbetsplatsen.

# Misstänkta försändelser

**Vid misstänkt försändelse** eller om paketet ser märkligt ut och där avsändaren är okänd; rör eller öppna inte och kontakta Polismyndigheten.

# Hantering av hotbrev

**Hantera eventuella hotbrev** med försiktighet och förvara dem skyddat så att polisen kan säkra eventuella spår och ta del av innehållet för att analysera det. Öppna inte i de fall flera försändelser kommer från samma avsändare. Analyser kan exempelvis ske genom att studera innehållet i texten och genom att säkra fingeravtryck. Även biologiska spår kan hittas på brevet. För att undvika att många hanterar hotbrevet är ett råd att ta ett foto på det istället för att hantera det ursprungliga brevet.

# Utpressning, stalkning och rättshaveristiskt beteende

I samband med ett politiskt uppdrag eller samhällsengagemang kan det finnas en risk att bli trakasserad på olika sätt av okända personer. Detta kan exempelvis ske genom oälkomna telefonsamtal, påhälsningar, brev, e-post eller via sociala medier.

## Utpressning

**Det förekommer att** personer vill störa det demokratiska beslutsfattandet genom utpressning. Utpressaren kan använda olika metoder för att tvinga till sig något eller för att ett beslut ska fattas i en viss riktning. Det kan röra sig om hot och ibland kan förtäckta insinuationer räcka för att skrämmas. En utpressare kan även utnyttja hållhakar eller svagheter. Ett generellt råd är att ha kontinuerliga samtal med säkerhetsansvariga i sin organisation och uppdatera dem om det sker något i privatlivet som kan utnyttjas av någon med onda avsikter. Om återkommande samtal kring den personliga säkerheten gjorts blir även råden bättre. Kontakta säkerhetsansvariga vid utpressning som är relaterad till det politiska uppdraget.

**Myndigheter, företag och** organisationer 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 polisen inte ska blandas in. Om en sådan situation uppstår, fundera noga på hur kommunikation med Polismyndigheten och andra berörda kan ske utan att bli upptäckt. I dessa situationer är det viktigt att hålla informationen i en så liten krets som möjligt.

# Stalkning

**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 är en brottsrubricering som innebär 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.

**Om känslan finns** av att vara förföljd och hotad av någon är det viktigt att detta anmäls både till Polismyndigheten och till den säkerhetsansvarige på arbetsplatsen eller organisationen. Det är även viktigt att det görs en bedömning av individen som gör detta. Bedömningen om individen utgör ett hot mot den utsattas säkerhet eller mot familjen görs av Polismyndigheten eller Säkerhetspolisen. Polismyndigheten och åklagare gör även en bedömning av vilka skyddsåtgärder som behövs. Detta bör ske i samverkan med den säkerhetsansvarige på arbetsplatsen eller i organisationen. Ett juridiskt biträde eller en motsvarande person kan vara ett stöd. Den personen kan även ha möjlighet att medverka i planeringen av åtgärder.

**Råd vid stalkning**

- ☐ Var tydlig med att inte vilja ha någon kontakt med individen ifråga när beteendet upplevs som obehagligt. När det är gjort, svara inte på vidare kommunikationsförsök. Varje kontakt innebär en risk för en positiv förstärkning för gärningspersonen och ökar risken för fortsatt oönskad förföljelse och då med ökad intensitet.
- ☐ Finns det stödfunktioner som tar emot e-post, inkommande samtal eller som modererar sociala mediekonton måste ett resonemang föras också med de funktionerna om hur hot hanteras.
- ☐ Gör en polisanmälan. Varje gång.
- ☐ Anmäl till säkerhetsansvariga på arbetsplatsen. 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 Polismyndigheten och andra professionella för att få råd kring möjlighet att agera.

# Personer med rättshaveristiskt beteende

**De som arbetar** inom offentlig sektor kan någon gång ha varit i kontakt med en person med ett rättshaveristiskt beteende 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. Att bli utsatt för en rättshaverist eller annan förföljelse kan resultera i omständigheter där alternativa uppdrag eller arbetsuppgifter kan behövas. I första hand ska den egna organisationen och säkerhetsorganisationen kopplas in, men om behov uppstår kontakta Polismyndigheten eller Säkerhetspolisen för att diskutera eventuella lösningar på problemet. Faktorer som inverkar på bedömningen och de åtgärder som genomförs är om hotet är personligt riktat eller enbart mot en funktion och arbetsuppgifter, men också hur situationen upplevs. För sådant arbete som kan medföra risk för våld och hot ska det finnas särskilda säkerhetsrutiner.

**Personer med rättshaveristiskt beteende**

- ☐ Ha en handlingsplan för hur ni ska hantera en upprörd, arg eller hotfull person.
- ☐ 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 som går att 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 det egna området.
- ☐ Förstå att det inte går att förändra personens åsikter. Ifrågasätt inte vanföreställningar.
- ☐ Vid långvarig eller komplicerad kontakt, prova med en annan handläggare eller kollega.
- ☐ Låt personen i fråga få sista ordet, kommentera inte ytterligare.
- ☐ Avsluta eller avbryt samtal som blir alltför kränkande, hotfulla eller meningslösa.

# In- och utrikes resor

Det är ovanligt med allvarliga hotsituationer vid resor, men terrorattacker runt om i världen har skapat en större säkerhetsmedvetenhet. Riskerna vid en resa kan variera liksom hur säkerheten ser ut dit resan går. Gör därför en bedömning av resmålet och eventuella säkerhetsåtgärder redan innan resan.

Om oro finns för att utsättas för angrepp i någon form under resan, välj en trygg omgivning och förbered en alternativ handlingsplan. Det gäller oavsett om resan sker inom landet eller utomlands och oberoende av färdsätt. Resor sker ofta i nya miljöer. Vid exempelvis restaurangbesök, var uppmärksam på vilka utgångar som finns utöver entrén. Välj om möjligt en plats långt in i lokalen med uppsikt över rummet. Försök att bedöma omgivningen och människorna i närheten.

### Innan avresa

**Innan avresa informera också enligt rutinerna berörda på arbetsplatsen och anhöriga om:**

- ☐ Ankomst och återresa.
- ☐ Resmål samt kontaktuppgifter. Meddela om det blir några förändringar för att snabbt kunna nås.
- ☐ Hur resan ska ske och vilka aktiviteter och programpunkter som är planerade, särskilt om de är kontroversiella.
- ☐ Vem eller vilka som ska träffas.

**Tänk även på att:**

- ☐ Res inte ensam om det känns otryggt.
- ☐ Lägg in nödnumret 112 eller det nödnummer som är aktuellt i det land där du befinner dig i din mobiltelefon så att du snabbt kan larma.
- ☐ Undvik att informera okända personer om resedetaljer.
- ☐ Ha gärna med en kopia på passhandlingen och extra foton, och förvara dem åtskilda från passet.

## 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. Konflikter i landet eller situationer i omvärlden kan påverka säkerheten under resan. Se till att ha en alternativ plan om det oförutsägbara skulle inträffa. Redan innan resan är det dessutom bra att bedöma om det är lämpligt att åka och vilka eventuella säkerhetsåtgärder som bör vidtas för att minska riskerna på plats. Denna bedömning bör göras i samråd med organisationen eller säkerhetsansvariga på arbetsplatsen.

**På Utrikesdepartementets** webbplats finns reserekommendationer som innehåller råd för olika länder när det gäller till exempel säkerhets- och hälsoläget i landet eller information om olika krissituationer. Reserekommendationerna finns på www.ud.se/resklar. Här finns även viktiga telefonnummer som går att ladda ner direkt till mobilen. UD har även en app, UD Resklar, där den viktigaste informationen om varje land finns.

## Allvarliga händelser utomlands

**Att svenska medborgare** i utlandet utsätts för utpressning eller hamnar i gisslansituationer är ovanligt. Men det kan hända och ställer stora krav på uthållighet, kunskap och förmåga att hantera den uppkomna situationen. Ha med telefonnummer till den svenska ambassaden eller konsulatet i landet för att få råd och hjälp vid en nödsituation. Om det saknas svensk representation i landet går det att vända sig till ett annat nordiskt lands eller EU-lands ambassad eller konsulat. Informera anhöriga vid resa till ett land med dålig mobiltäckning och om möjligt, hör av dig regelbundet.

**Bevaka kontinuerligt** händelser som rör staden eller platsen samt politiska händelser i världen som kan påverka säkerheten på resmålet. 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. Var därför informerad om hur det ser ut i det land dit resan går samt observant för att upptäcka och undvika tänkbara riskmoment. Var förutseende och ha medicin eller recept lättillgängliga vid sjukdom. Detta kan minska sårbarheten vid hastigt uppkomna situationer. Ha med aktuella telefonnummer till anhöriga, arbetsgivare och försäkringsbolag.

## Risker vid flygresor

**Vid flygresor utomlands** är det viktigt att vara uppmärksam på omgivningen och hålla bagaget under noggrann uppsikt. Det kan även vara bra att vara på plats i god tid innan avresan på grund av den ökade säkerheten på flygplatser. Väl där, gå innanför säkerhetskontrollen då risken för attentat är avsevärt högre i vänthallen. Genom att packa rätt så att inte problem uppstår i säkerhetskontrollen minskas risken för exponering. Försök att välja en väska utan fickor på utsidan då någon kan placera något föremål i den. Lämna aldrig det egna bagaget till någon annan eller utan uppsikt – från packning till incheckning. Slutligen, ha heller inte någon utvändig märkning med anknytning till arbetsplats om det kan vara känsligt, till exempel organisations- eller partiemblem på bagage, kläder, väskor eller liknande.

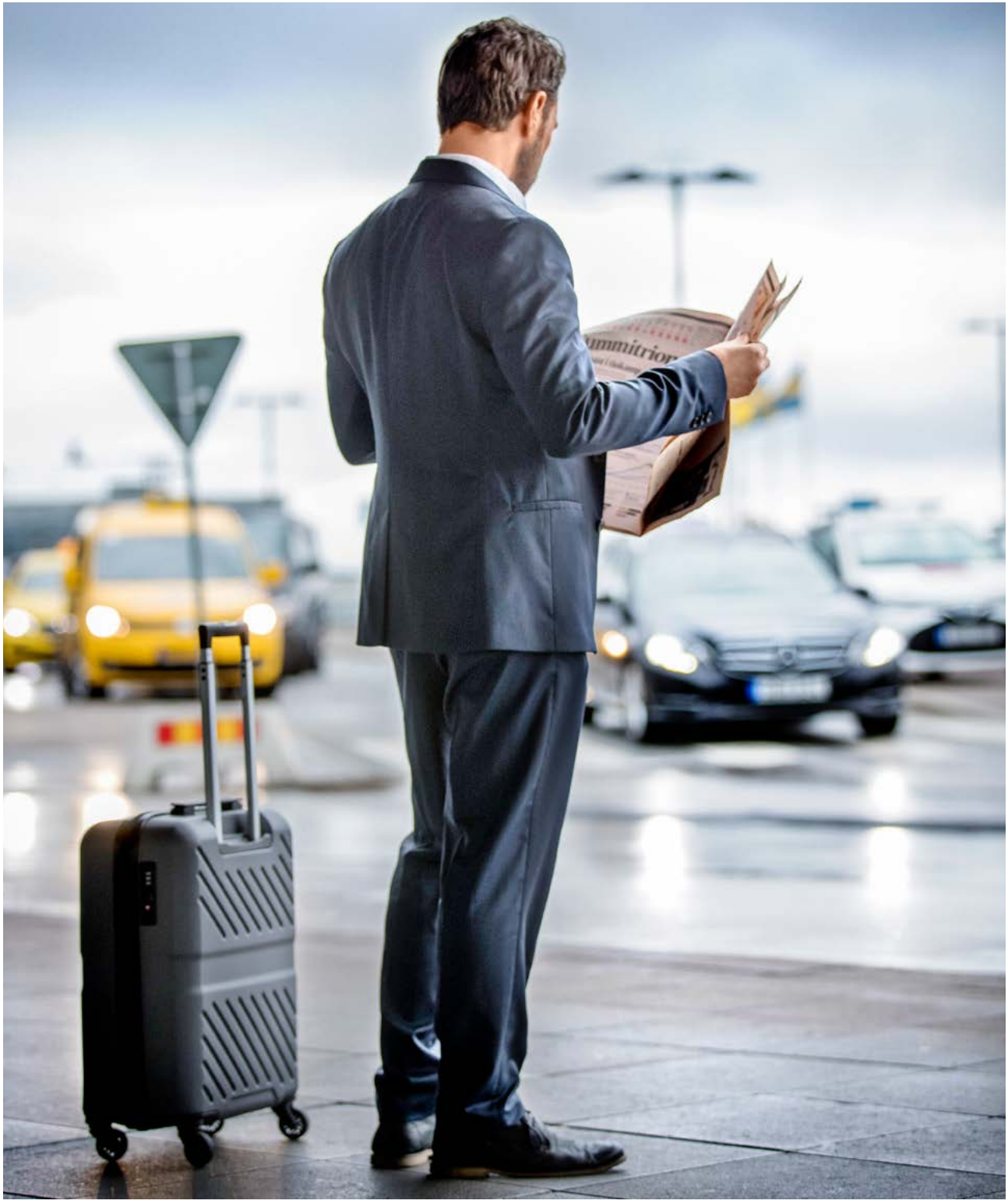
**Tips under resor**

- ☐ Om byten ska ske under resan, boka dem i lågrisländer.
- ☐ Anländ till resmålet under dagen eftersom det kan vara svårare att få taxi eller annan hjälp samt att risken för kriminalitet är större kvälls- och nattid.
- ☐ Säkerställ att du kan höra viktig information på flygplatser samt kan få eventuell förvarning vid en incident. Ha därför inte på hörlurar. Samma råd gäller under färd med allmänna kommunikationer vid förhöjd terrorhotnivå.
- ☐ Placera teknisk utrustning i handbagaget.

## Underrättelseinhämtning under utrikesresan

**Att bli kartlagd** eller utsatt för underrättelseinhämtning under utrikesresan är en potentiell risk. Den som vill kartlägga någon vill komma över information. Det kan vara fakta, men också kontakter eller samverkanspartners. Utifrån främmande makts 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 bussar och tåg, konferenser, mässor och i hotellreceptioner.

**Det finns dock** ett antal åtgärder som kan vidtas för att försvåra för främmande makt. Ryssland, Kina och Iran är de länder som utgör det största underrättelsehotet mot Sverige, men det finns även andra länder som har intresse av Sverige. Överväg vilken teknisk utrustning som behöver vara med under resan. Ta bara med sådant som är absolut nödvändigt. Tänk på att myndigheterna i vissa länder har rätt att kontrollera innehållet i teknisk utrustning i samband med gränspassage. Förutsätt att fysiska utrymmen samt tele- och datatrafik avlyssnas. Diskutera inte känsliga ämnen i exempelvis taxin eller på hotellrummet. Överväg, beroende på resmål, att använda en särskild telefon och bärbar dator som enbart är avsedd för den specifika resan. Använd aldrig elektronisk utrustning som ges i gåva, exempelvis USB-stickor eller laddare. Undvik även att vistas ensam ute under kvällar och nätter. Det kan finnas risk för närmanden från främmande makt i exempelvis restaurang- och barmiljöer.



## Transfer och taxiresor

**Oavsett om en** chaufför hämtar upp från flygplatsen eller om taxi tas, säkerställ att dörrarna är låsta vid färd. Trafiken kan vara en av de största riskerna. Ta därför reda på vilka taxibolag som är tillförlitliga och var inte rädd för att be chauffören dra ner på farten om det går för fort. Det är även viktigt att alltid använda bälte. Om det saknas, byt bil. Åk aldrig taxi med någon som har okända ”medpassagerare”. Ha gärna en utskrift på hotell och destination för att undvika missförstånd. Förbetala taxifärden om möjligt, men annars inne i bilen. Ring gärna en kollega eller en partnerorganisation och meddela att ni är på väg, speciellt om resan känns obehaglig. Håll samtalet igång så länge det behövs och fråga chauffören när ni beräknas vara framme.

**Om taxiliknande tjänster** som bokas via appar används, var noga med att kolla att registreringsnumret, bilmodellen och föraren stämmer med den information som finns i appen. I vissa av dessa tjänsters appar finns även en nödhjälpsknapp som kan användas för att ringa efter hjälp. Genom att använda sig av den funktionen får räddningstjänsten tillgång till positionen samt information om resan.

**Vid upphämtning av chaufför**

- ☐ Se till att få chaufförens namn och nummer i förväg.
- ☐ Lämna även det egna numret 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.

## Säkerhet på hotellet

**Välj ett säkert** boende genom att exempelvis höra med kolleger om någon av dem varit på platsen tidigare. Överväg om det är nödvändigt att lämna ut e-postadress vid incheckning. En sådan trivial sak som att nämna sitt rumsnummer kan vara av intresse vid personlig kartläggning. 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 det egna arbetet, personlig information, information om familjen eller teknisk utrustning på hotellrummet. Betrakta inte hotellets säkerhetsskåp som säkert. Om utrustningen måste lämnas utan uppsikt, använd en så kallade säkerhetspåse för hantering av värdefullt eller känsligt innehåll. Om något inte känns bra med rummet, våningsplanet eller om uppgifter om rumsnummer eller liknande kommit ut, var inte rädd för att insistera på att få byta rum. Precis som i vanliga fall är det bra att överväga vilken information som läggs ut i sociala medier. Den politiska situationen eller det lokala sammanhanget kan dessutom ha betydelse för hur kommentarer och inlägg uppfattas.

# Terrorangrepp och andra attentat

Sannolikheten att drabbas av attentat i form av politiskt eller religiöst våld är liten, men det är ändå viktigt att känna till bästa sätt att agera om ett angrepp eller motsvarande våldsbrott skulle inträffa oberoende om det sker i Sverige eller utomlands. Ett sätt att vara mentalt förberedd är att föreställa sig olika scenarier och situationer, samt olika sätt att agera.

Den mentala förberedelsen kan vara avgörande eftersom den tid det tar att förstå vad som händer kan vara vital för att hinna ta sig ur situationen. Var uppmärksam på nödutgångarna i offentliga eller andra publika miljöer där ett dåd kan ske. 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.

## Tre steg vid terrorattentat

### 1. Fly

- ☐ Fly från platsen och sätt dig själv i säkerhet.
- ☐ Var förberedd på att ytterligare attentat kan ske.

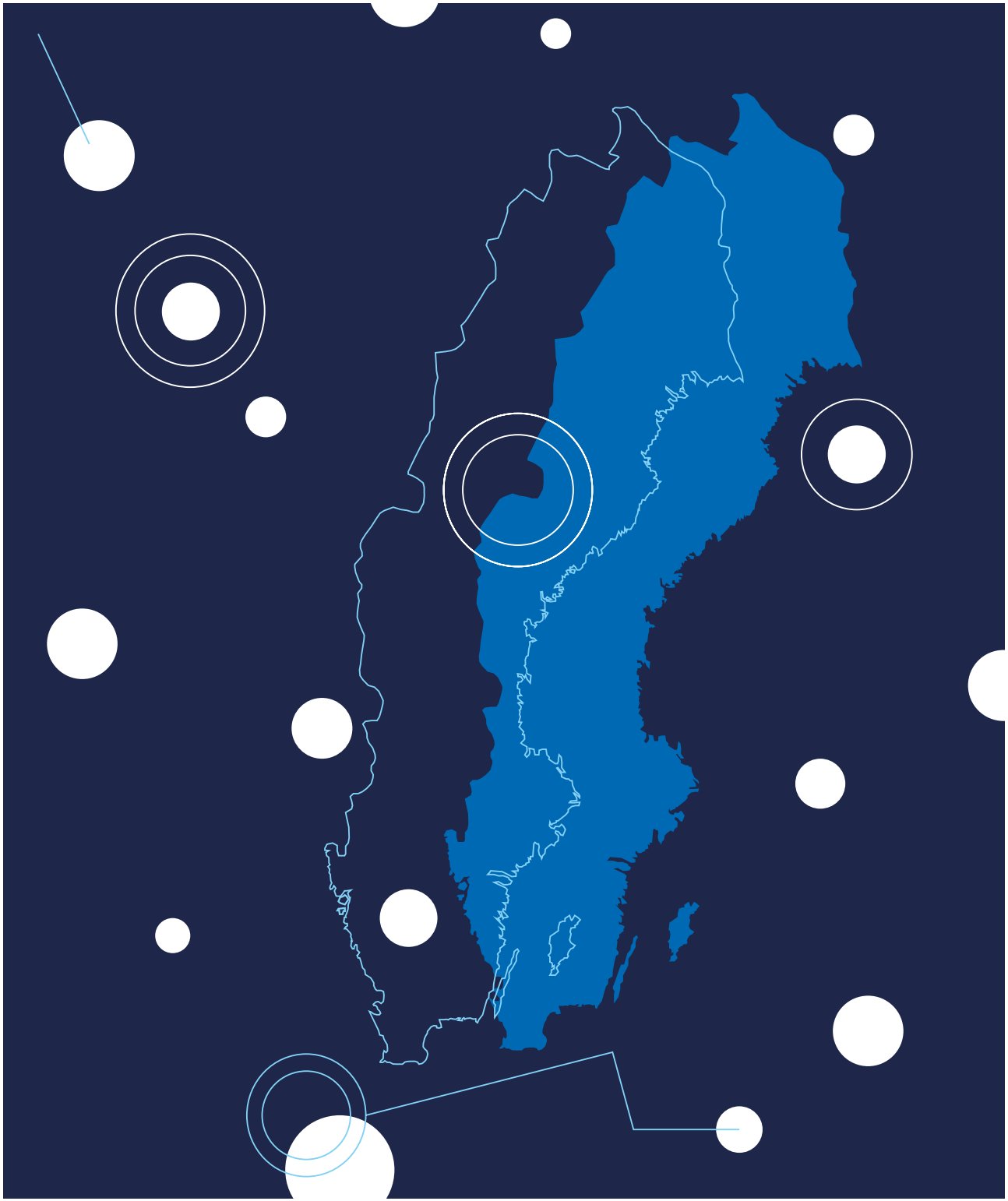
### 2. Sök skydd

- ☐ Om det inte går att fly, hitta ett säkert gömställe som går att låsa eller blockera. Undvik fönster och dörrar tills faran är över.
- ☐ Lås, släck ljuset och var tyst.
- ☐ Slå av ljudet på mobiltelefonen.
- ☐ Ring inte i onödan till personer som kan befinna sig i riskområdet, det kan utsätta dem för fara.
- ☐ Lämna inte ett säkert område för att se vad som händer. Gå inte tillbaka förrän polisen eller militären har gjort platsen säker.
- ☐ Var alltid beredd på en ny attack och följ de råd som polis eller militär samt räddningstjänst ger.

### 3. Larma

- ☐ Ring/larma så fort möjlighet ges.
- ☐ Det är polisens alternativt militärens uppdrag att avbryta ett pågående attentat, beroende på i vilket land det sker. För att de 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 uppmaningar. När polisen eller militären kommer till platsen, se till att inte misstas för att vara gärningsman. Håll därför inget i händerna.

**+** Tips! Läs mer på Polismyndighetens webbplats www.polisen.se.



# Källhänvisning

Boken Personlig säkerhet har tagits fram av Säkerhetspolisen i samarbete med Polismyndigheten.

Delar av informationen i boken har inhämtats i samråd med:
Myndigheten för samhällsskydd och beredskap, msb.se
Integritetsskyddsmyndigheten, imy.se
Internetstiftelsen, internetkunskap.se
Skatteverket, skatteverket.se
Transportstyrelsen, transportstyrelsen.se
SOS Alarm, sosalarm.se

**Produktion:** Säkerhetspolisen, fjärde upplagan 2021
**Grafisk form:** Springtime Intellecta
**Foto:** TT-bilder, Ulf Huett, Johnér bildbyrå
**Typografi:** Eurostile och Palatino
**Papper inlaga:** 120 g obestruket Papper omslag: 300 g obestruket
**Tryck:** Stibo Complete
**ISBN-nummer:** 978-91-86661-21-2

Det är Säkerhetspolisens ansvar att det som inte får hända, inte heller händer. Därför arbetar vi förebyggande. Vi avvärjer hot mot Sveriges säkerhet och mot medborgarnas fri- och rättigheter. För vårt uppdrag är att säkra framtiden för demokratin. Och vi utför uppgiften handlingskraftigt och långsiktigt. Vi skyddar centrala statsledningen och Sveriges hemligheter. Vi motverkar spionage, extremism och terrorism. För oss är de viktigaste händelserna de som aldrig inträffar.

Säkerhetspolisen

Box 12312, 102 28 Stockholm
010-568 70 00 | sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se