Säkerhetspolisen

Personlig säkerhet

Med ett allvarligt säkerhetsläge och en orolig omvärld behöver vi arbeta tillsammans för att bygga säkerhet. Som politiker och offentlig person behöver du göra medvetna val för att höja din säkerhet.

Innehåll

Vi bygger säkerhet tillsammans

Säkerhetspolisens uppdrag är att skydda Sveriges säkerhet. En uppgift är att skydda den centrala statsledningen. Med ett allvarligt säkerhetsläge och en orolig omvärld behöver vi arbeta tillsammans för att bygga säkerhet. Som politiker och offentlig person behöver du göra medvetna val för att höja din säkerhet.

Hotet från främmande makt och antidemokratiska krafter utmanar vårt samhälle. Varje dag sker försök att stjäla uppgifter av betydelse för Sveriges säkerhet och att påverka svenskt beslutsfattande. Angreppen riktar sig mot många olika delar i vårt samhälle och hotar både grundläggande fri- och rättigheter och vårt politiska oberoende.

Säkerhetspolisens uppdrag är att förebygga, förhindra och upptäcka hot mot Sveriges säkerhet. Tillsammans med bland andra Polismyndigheten och säkerhetsansvariga funktioner arbetar vi för att politiker i riksdag och regering ska ha möjlighet att utföra sina uppdrag utan att utsättas för hot eller våld.

Som enskild politiker behöver du tänka på säkerhet ur flera perspektiv. Ditt agerande gör stor skillnad. Genom riskanalyser, aktiva val och medvetna förhållningssätt kan du värna om din personliga säkerhet. Denna handbok är ett stöd i det arbetet.

Handboken innehåller råd och stöd till politiskt aktiva, men kan också användas av andra yrkesgrupper. Här finns exempel på säkerhetsåtgärder för att förebygga och hantera hotfulla situationer som kan uppstå. Här finns också råd om allt från sociala medier och teknisk utrustning till säkerhet i hemmet och resor utomlands.

Med handboken vill Säkerhetspolisen öka säkerhetsmedvetandet. Råden ska ses som en grund för din personliga säkerhet. Under vissa omständigheter kan ytterligare åtgärder behövas. Det gäller också om du har en särskilt utsatt position.

Risken att bli utsatt ser olika ut från person till person, från uppdrag till uppdrag och från tid till annan. Gemensamt är att det är ett hot mot Sveriges demokrati om folkvalda politiker inte kan utföra sitt uppdrag. Vi behöver arbeta tillsammans för att bygga säkerhet.

Läs handboken på webben

På sakerhetspolisen.se/personlig-sakerhet hittar du onlineversionen av handboken ”Personlig säkerhet”.

1

Säkerhet vid politiskt arbete

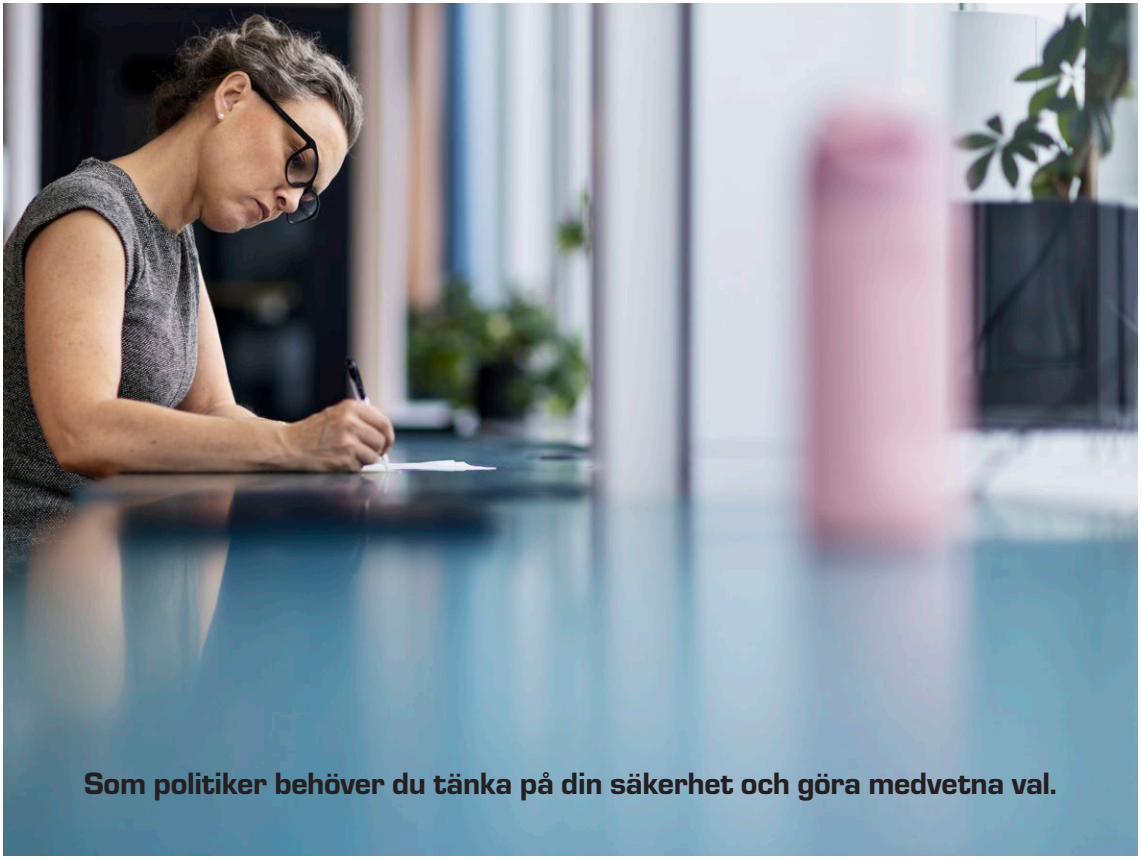
Det finns aktörer som vill begränsa den demokratiska processen. Orsakerna är flera, men konsekvensen kan bli att grundläggande demokratiska funktioner hotas.

Det är viktigt att politiker kan utöva det demokratiska uppdraget under säkra former. Beroende på vilken nivå en politiker verkar inom har antingen Säkerhetspolisen eller Polismyndigheten ansvar för att bedöma hot och skyddsåtgärder. Det kan handla om information och rådgivning, tekniska skyddsåtgärder som lås och larm, eller personbevakning där den yttersta åtgärden är livvaktsskydd.

Det är lika viktigt att enskilda politiker och deras organisationer regelbundet själva lyfter säkerhetsfrågor och genomför utbildningar. Egna riskanalyser och ett medvetet förhållningssätt bidrar till ökad säkerhet.

Oavsett vem som tar hand om skyddsåtgärderna ska de utformas utifrån varje enskild situation efter en noggrann bedömning av sårbarheter och risken för hot och angrepp.

Att ha ett politiskt uppdrag som förtroendevald innebär en förändring i vardagen. Du behöver vara medveten om säkerhet och göra anpassningar. Ha en dialog med säkerhetsansvarig i din organisation för stöd kring det.



Som politiker behöver du tänka på din säkerhet och göra medvetna val.

Skydd av person – vem ansvarar?

Säkerhetspolisen
ansvarar för att bedöma hot och skyddsåtgärder för den centrala statsledningen. I den ingår statschefen, tronföljaren, talmannen, riksdagsledamöterna, statsministern, statsråden liksom statssekreterarna och kabinettssekreteraren. Säkerhetspolisen utreder brott mot den centrala statsledningen som har ett politiskt motiv och där våld, tvång eller hot förekommer.

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

Enskilda politiker och tjänstemän
behöver göra egna bedömningar och medvetna val, i samarbete med säkerhetsansvariga i den egna organisationen.

2

Hotet från främmande makt

Främmande makt bedriver kontinuerligt säkerhetshotande verksamhet i och mot Sverige, bland annat genom att hämta in information och utöva påverkan. Det pågår här och nu. Politiker är en målgrupp som riskerar att utsättas.

Främmande makts underrättelseverksamhet riktar sig mot flera delar av samhället och sker med flera olika metoder. Genom bland annat kartläggning, värvning av agenter, cyberangrepp och signalspaning försöker främmande makt få tillgång till information som kan skada Sverige och svenska intressen om motståndaren får tag på den.

Ett sms eller mejl med en länk, eller ett trevligt samtal med någon som säger sig vara journalist, lobbyist eller forskare, kan vara ett försök till underrättelseinhämtning. Både privat och tjänsterelaterad information kan en motståndare utnytttja för att utöva påtryckningar, hot och tvång.

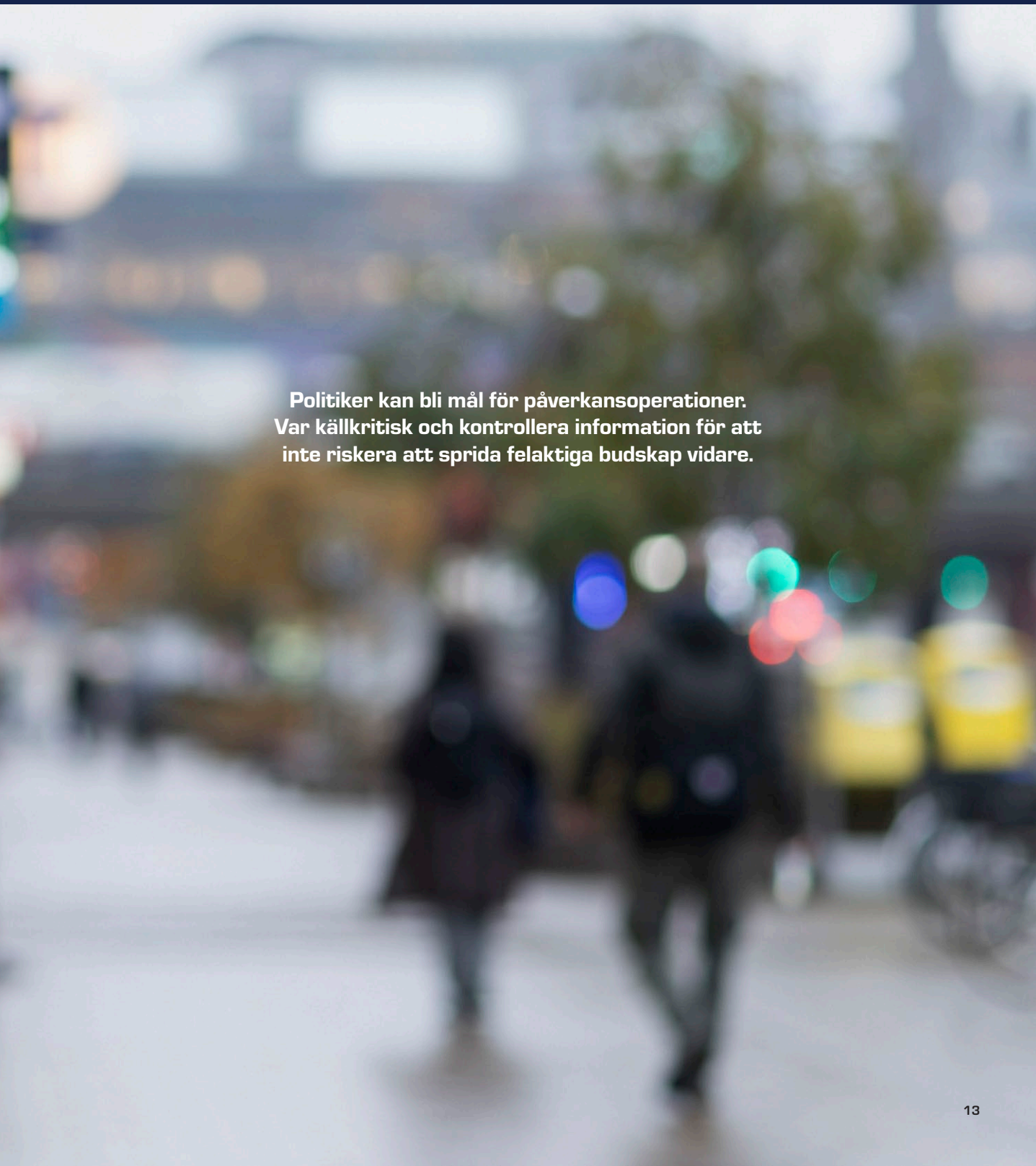
För att inte utsättas behöver du vara uppmärksam och själv kunna avgöra vilka som är behöriga att ta del av olika uppgifter. Säkerhetsansvariga i din organisation kan hjälpa till i det arbetet. Finns misstanke om att du har varit utsatt för exempelvis underrättelseinhämtning eller påverkan ska du rapportera till säkerhetsansvarig som i sin tur kontaktar Säkerhetspolisen.

Påverkansoperationer

Främmande makt, antistatliga rörelser och våldsbejakande extremister sprider desinformation, konspirationsteorier och propaganda i bland annat sociala medier. Syftet är att gynna sina egna intressen genom att till exempel skapa motsättningar och öka misstron mot det svenska samhället.

Politiker kan bli mål för koordinerade kampanjer, så kallade påverkansoperationer. Det kan handla om försök att påverka beslut, uppfattningar eller beteenden hos den centrala statsledningen, befolkningen eller utvalda målgrupper. Därför är det viktigt att vara källkritisk och kontrollera information för att inte sprida felaktiga budskap vidare, vilket kan öka motsättningar och påverka din personliga säkerhet.

Läs mer om källkritik i kapitel 4 ”Traditionella och sociala medier”.



Politiker kan bli mål för påverkansoperationer. Var källkritisk och kontrollera information för att inte riskera att sprida felaktiga budskap vidare.

Så värvas en agent

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

Steg 1 – Analys
Den utländska underrättelsetjänsten gör en analys av vilken information de 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
Den utländska underrättelsetjänsten kartlägger personen som bedöms ha tillgång till rätt information. Uppgifter om personliga egenskaper, svagheter, ekonomi och familjesituation ligger till grund för att bedöma 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 om det i själva verket är mycket välplanerat. Det kan både ske fysiskt eller i digitala miljöer.

Steg 5 – Vänskap
Efter att kontakten är etablerad försöker underrättelseofficeren inleda en vänskapsrelation med den tilltänkta agenten (spionen). I den här fasen får den utvalda personen oskyldiga uppdrag för att testa relationen. Det kan handla om att bli ombedd att dela information som inte är hemlig. 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 går enligt plan har personen blivit agent för ett annat lands underrättelsetjänst.

Personliga möten i syfte att värva

Genom underrättelseofficerare försöker främmande makt att rekrytera personer, så kallade agenter, som har tillgång till information eller ingår i ett nätverk av personer som är av intresse för främmande makt, i syfte att samla information om Sverige och svenska förhållanden.

Främmande makt arbetar ofta långsiktigt. Som politiskt aktiv kan du bli uppsökt, fysiskt eller digitalt, av exempelvis bekantskaper från tidigare i karriären. Mötet kan verka vara en tillfällighet, men om personen som sökt upp dig efter en tids återupptagen kontakt börjar intressera sig i detalj för det politiska uppdraget och vill få information bör du bli misstänksam. Det kan vara en del av en fas i en långsiktig plan där främmande makts utsända söker vänskapsband med någon för att så småningom få personen att lämna ut information. Det yttersta målet kan vara att värva dig som agent.

Tänk på att alla kan vara potentiella mål för värvningsförsök, det handlar om vem som kan ha eller skaffa sig tillgång till önskad information. Det innebär att även personer i närhet till någon med tillgång till säkerhetsklassificerad information kan utsättas för värvningsförsök. Upplever du att någon tar misstänkt kontakt eller försöker värva dig ska du kontakta säkerhetsansvarig i din organisation och Säkerhetspolisen.

På sakerhetspolisen.se kan du lämna information under ”Tipsa oss”.

Om du utsatts för ett misstänkt värvningsförsök

- ☐ Notera vem som gjorde kontaktförsöket, när och hur det gick till samt vilken anledning personen uppgav till kontakten.
- ☐ Ta kontakt med säkerhetsansvarig i din organisation och Säkerhetspolisen.

3

Kampanjarbete och offentliga möten

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

Ett första steg i säkerhetsarbetet inför kampanjarbete och offentliga möten är att göra en riskanalys, att rådgöra med säkerhetsansvariga om befintliga rutiner, att 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 du identifierar risker och bedömer vilka åtgärder som behöver vidtas för att undvika eller minimera riskerna. En riskanalys kan också vara mer detaljerad och omfatta särskilda aktiviteter eller säkerhetsåtgärder för en specifik situation. Ett exempel kan vara säkerhetsåtgärder inför en lång resa, som att larma hemmet, ge anhöriga adresser och resplaner och att förvara pass och resehandlingar säkert.

Som politiskt engagerad behöver du regelbundet reflektera över och analysera risker och sårbarheter. Det är viktigt att försöka bedöma eventuella konsekvenser och reaktioner på till exempel beslut som ska fattas eller planerade uttalanden. För stöd i detta kan du ta hjälp av säkerhetsansvarig och kommunikationsansvarig i din organisation.

Se checklista "Riskanalys vid offentligt möte" på sidan 21.

Möten med allmänheten

När man planerar ett torgmöte och ska placera en scen eller ett talarpodium, är det viktigt att tänka på att talaren har ryggen fri. Det går att ordna med exempelvis en skyddad bakgrund eller fond.

Undvik placering på en yta där folk kan stå runt omkring. Tänk på risken för angrepp från personer och hur långt avstånd det är att eventuellt kasta något fram till scenen. Det går att skapa säkerhetsavstånd till talaren på olika sätt, till exempel genom att sätta upp rep, band eller blommor. Det försvårar för en angripare att snabbt nå talaren och ger värdefull tid för förvarning. Det medför i regel även att folk ser bättre. Vid sittande publik går det att reservera första raden för till exempel media eller särskilt inbjudna gäster.

Tänk på var entréer placeras och var vakter, funktionärer och eventuella journalister kan stå. Om publiken ska kunna ställa frågor i mikrofon är det viktigt att inte släppa den. Låt istället en medarbetare hålla mikrofonen åt den som vill ställa en fråga, för att behålla kontrollen. Om någon kommer fram för att ge en gåva bör givaren helst packa upp den själv.

Ha beredskap för störningar

För att kunna hantera incidenter och spontana störningar under ett evenemang är det viktigt att förbereda i god tid. Det kan handla om att fördela roller på plats och att upprätta bra kommunikationsvägar till dem som ska bevaka arrangemanget. Om någon stör eller uppträder hotfullt under ett evenemang är det bäst att försöka undvika att provocera personen. Lägg in nummer till viktiga kontakter såsom polis eller väktare i mobilen. Om ett akut läge uppstår, ring 112.

Steg i en riskanalys

Vad
behöver analyseras särskilt? Vilka aktiviteter? 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?

När och var
är det störst risk för att bli utsatt för ett påhopp eller angrepp?

Hur
kan man minska risken eller konsekvensen? Vilka åtgärder kan vidtas? Går det att ta skydd vid en hotfull situation? Går det att larma och snabbt få hjälp om något skulle hända?

(!) Tänk på
Hotfulla situationer kan ha sin upprinnelse i händelser som ligger långt tillbaka i tiden.

Planera vägen ut

Planera vägen ut genom att lokalisera nödutgångar. Ha en reträttväg klar till en säker plats om något händer och en säker parkeringsplats i nära anslutning till scenen. Identifiera säkra rum att söka skydd i, helst med låsbara dörrar och utan insyn, om det offentliga mötet hålls i en lokal. Undvik också om möjligt 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

Politiskt aktiva deltar ofta i olika kampanjer. När du knackar dörr finns det flera saker att tänka på för att genomföra det så säkert som möjligt.

Se checklista ”Säkerhet vid dörrknackning” på sidan 21.

Säkerhet vid bilfärder

Bilen kan vara en säker plats 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 vid en hotfull situation. Kommunicera istället genom bilrutan, kalla på hjälp eller ta dig till en plats där det finns andra människor. Lås alltid dörrarna under bilfärd.

Misstänker du att någon typ av kartläggning skett är det bra att variera färdväg och restider. Vid förhöjd hotbild är rådet att du använder säkra parkeringsplatser, exempelvis ett väl skyddat garage utan koppling till bostadsadressen.

Billarm kopplade till bilens låsfunktion används för att motverka skadegörelse och stöld och för att se om någon har öppnat eller rört bilen. Det är viktigt att du alltid förvissar dig 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 och taxinumret vid taxiresa. Betala om möjligt i förväg via en app, eftersom det gör att du snabbare kan ta dig 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 du bokar taxi via app, var noga med att kolla att registreringsnumret, bilmodellen och föraren stämmer med informationen i appen.

Riskanalys vid offentligt möte

- ☐ Bedöm om något kan påverka hur mötet bör genomföras. Påverkar deltagare/ämnet/platsen/lokalen säkerheten? Ska en kontroversiell fråga diskuteras eller är platsen särskilt utsatt?
- ☐ Gå igenom schemat och identifiera platser eller situationer där det är störst risk för angrepp.
- ☐ Undersök om obehöriga kan ta reda på information som ökar risken för ett angrepp, till exempel om skyddet har synliga brister eller om förbipasserande har insyn som ger överblick.
- ☐ Ha en plan för hur säkerhetsansvariga ska agera vid oförutsedda händelser eller störningar.
- ☐ Bedöm vilka resurser och bevakningsåtgärder som krävs för säkerheten. Samverka med Polismyndigheten eller Säkerhetspolisen, beroende på vem som har ansvar. Skaffa information om tillstånd för allmänna sammankomster via Polismyndigheten. Informera Polismyndigheten om eventuellt kontroversiella budskap.
- ☐ Ta reda på om Polismyndigheten känner till andra evenemang, till exempel om en demonstration ska hållas parallellt med mötet.
- ☐ Bedöm i god tid vilken information som ska gå ut inför mötet, till exempel vilka uppgifter om mötet som kommuniceras i sociala medier. Var noggrann med vilka som får veta detaljerna i programmet. Undvik att sprida uppgifter till obehöriga om ankomsttid till hotell, när middag ska intas och liknande.

Säkerhet vid dörrknackning

- ☐ Sök information om området du ska besöka i god tid innan besöket.
- ☐ Ha med mobiltelefon och bärbart larm om du har ett.
- ☐ Håll reda på var du befinner dig om du behöver tillkalla hjälp.
- ☐ 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 inom synhåll.

4

Traditionella och sociala medier

Att medverka i medier och använda sociala medier är en självklarhet för många förtroendevalda för att nå ut med budskap och interagera med väljarna. När du gör det är det också viktigt att tänka på säkerheten.

Det är viktigt att fundera i förväg på vilka sammanhang och platser du visar upp och vilka uttalanden och kommentarer du gör i medier och sociala medier. Hemmet, familjen och miljöer du besöker regelbundet ska inte exponeras. Kommentera inte säkerhetsåtgärder du vidtar. Gör uttalanden och kommentarer med eftertanke utifrån säkerhetssynpunkt.

Undvik även att nämna arbets- eller partikamrater i intervjuer eller i kontakt med media om det inte är förankrat hos dem. Om det finns pressansvariga på arbetsplatsen eller i partiet kan du rådfråga dem vid osäkerhet. Vid minsta tveksamhet, kontakta den egna organisationen innan publicering. Hot ska polisanmälas.

Sociala medier

Sociala medier gynnar innehåll som manar till engagemang, reaktioner och debatter. Samtalstonen skruvas lätt upp i diskussioner.

Risken för att bli föremål för storskaliga och plötsliga kontroverser är särskilt hög om man är en offentlig person, såsom politiker, journalist eller opinionsbildare. Det är yrkesroller som driver frågor där många personer har starka åsikter. Du som är politiskt aktiv och din organisation behöver ha en handlingsplan för hur ni ska agera i sociala medier. Tonläget, och därmed eventuell hotbild, kan förändras och höjas på kort tid och ni kan snabbt behöva analysera, nyansera eller dementera uppgifter som cirkulerar. En handlingsplan kan också vara ett bra stöd vid beslut om eventuella säkerhetsåtgärder ifall situationen skulle bli allvarlig. Använd blockeringsfunktioner på tjänster vid behov och polisanmäl hot.

Tänk även på den personliga integriteten i sociala medier. Ett råd är att skapa en öppen offentlig sida i sociala medier som hålls avskild från din privata sida, där du helst ska ha stängd profil, det vill säga att profilen endast är synlig för personer du har godkänt. Var noga med att använda ett starkt lösenord, helst tvåfaktorsautentisering och att byta lösenord med jämna mellanrum. Då minskar du risken för att ditt konto blir kapat.

Skapa en genomtänkt hållning för vad, när och hur du kommunicerar i medier och sociala medier, utifrån ett säkerhetsperspektiv.

Källkritik

Vi nås av information från många olika källor, och det är inte alltid lätt att veta vad som är verkligt eller inte. Därför behöver du vara källkritisk till alla typer av innehåll, oavsett om det är text, ljud eller bilder.

Med AI går det att påverka innehåll på ett sätt som gör det mycket svårt att skilja på autentiskt och falskt material. Det går både att skapa nytt video- eller ljudmaterial och att byta ut exempelvis ansikten och röster i redan existerande material. Dessa förfalskningar, så kallad deepfake, gör det möjligt att klippa in en person i ett sammanhang som inte stämmer. Det kan användas för att vilseleda och sprida desinformation och kan även hända politiska företrädare. Var uppmärksam så att du själv inte utsätts eller utnyttjas. Ett kritiskt tänkande garanterar inte att du undviker att bli lurad, men gör dig mer medveten om riskerna.

Tips!
Läs mer om källkritik på Myndigheten för psykologiskt försvars webbplats mpf.se och Internetstiftelsens webbplats internetkunskap.se

Några källkritiska kontrollfrågor

- ☐ Vem är avsändaren? Kan du hitta den ursprungliga källan?
- ☐ Vad är det bakomliggande syftet med informationen? Är det propaganda eller information?
- ☐ Vem tjänar på att du sprider informationen? Har någon ett intresse av att vinkla uppgifterna?
- ☐ Hänvisas det till källor? Är dessa källor tillförlitliga?
- ☐ Finns det fler källor som säger samma sak och bekräftar informationen?
- ☐ Hur gammal är informationen? Är den fortfarande relevant och aktuell?

Vägledning i sociala medier

- ☐ Skapa en genomtänkt hållning för vad, när och hur du kommunicerar i sociala medier, utifrån ett säkerhetsperspektiv.
- ☐ Se över vad du exponerar, vilken sorts innehåll och foton du lägger ut. Publicera inte bilder där det går att identifiera bostadsadressen eller andra uppgifter om ditt privatliv.
- ☐ Berätta helst om möten och event som redan har skett, inte om sådant som ska ske. Det minskar risken att bli kartlagd eller uppsökt av personer.
- ☐ Använd inte funktioner som avslöjar den geografiska positionen om det inte är nödvändigt.
- ☐ Låt om möjligt utpekade medarbetare moderera kommentarer och meddelanden i dina publika konton istället för att läsa allt själv.
- ☐ Ta fram en handlingsplan för hur hot- och hatfyllda kommentarer ska hanteras. Ta gärna hjälp av kommunikationsavdelningen och säkerhetsansvariga i organisationen.
- ☐ Vid hot, skärmdumpa inläggen och kontakta i ett första steg säkerhetsansvariga i din organisation som i sin tur kan kontakta Polismyndigheten eller Säkerhetspolisen.
- ☐ Undvik att exponera eller ge en inblick i vanor såsom tränings- eller shoppingrutiner eller platser du regelbundet besöker.
- ☐ Fråga personer som medverkar i inlägg och på bilder om godkännande före publicering.
- ☐ Berätta även i privata sammanhang om vad som gäller för din egen medverkan i sociala medier. Be vänner och familj att undvika att ange geografisk plats, oavsett social medieplattform.
- ☐ Se över säkerhetsinställningar med jämna mellanrum och aktivera tvåfaktorsautentisering.
- ☐ 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.

5

Hantera hot och angrepp

Att vara förberedd på hot kan göra det lättare att agera korrekt. Du kan i förväg tänka igenom olika scenarier och handlingsalternativ för situationer som skulle kunna uppstå vid ett offentligt framträdande, på nätet, på arbetsplatsen eller vid bostaden.

En hotfull situation kan bland annat handla om påträngande personer, oönskade påhälsningar och gåvor. Hot kan också framföras via brev, telefon, mejl eller i sociala medier. Ett första råd är att försöka hålla sig lugn. Genom att vara uppmärksam på vad som händer kan du anpassa ditt agerande utifrån situationen och hur den förändras. Försök att vara saklig även vid provokationer. När du bemöter en person, försök få denne att bryta sitt handlingsmönster genom att föreslå alternativ till personens agerande.

Om en situation är hotfull gäller det att både bedöma avsikten hos personen ifråga och hur du behöver agera. Det kan handla om att ropa på hjälp, fly från platsen eller att försvara dig. Handla alltid med eftertänksamhet.

Hot på internet och telefon

En direkt reaktion på ett hotfullt meddelande kan vara att snabbt radera det. Men för att en utredning ska kunna bedrivas och någon lagföras är det viktigt att du inte raderar hot eller trakasserier som kommer in via mejl, sociala medier eller sms. De behövs bland annat för att kunna spåra var de har skickats ifrån. Vissa meddelanden raderas med automatik efter en viss tid eller om avsändaren väljer att ta bort det, beroende på plattform. Ta därför en skärmdump av det hotfulla meddelandet.

Hot eller trakasserier via telefon eller via internet bör snarast anmälas till säkerhetsansvarig i organisationen och Säkerhetspolisen alternativt Polismyndigheten beroende på vem som har utsatts för hotet. I en eventuell brottsutredning kan det gå att spåra vem som använt det aktuella telefonnumret eller IP-adressen.

Vad är ett hot?

Det händer att politiker får ta emot både hot och hat. Hat är obehagligt för den som utsätts men att skriva hatiska kommentarer till någon behöver i sig inte vara brottsligt. Hot behöver inte heller alltid vara ett brott, det beror på hur det är utformat. Om antalet hatfulla kommentarer eller liknande ökar bör du kontakta säkerhetsansvariga då det kan vara en indikation på en ökad hotbild. Ibland kan det vara svårt att skilja mellan hot och hat. Är du osäker om du utsatts för olaga hot eller inte, prata med säkerhetsansvarig och bedöm om agerandet ska polisanmälas.

Exempel på brott

Olaga hot

4 kap. 5 § brottsbalken

Olaga hot är 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 vara ett påstående om att ett brott kommer att utföras. Hotet kan till exempel avse våld mot person eller skadegörelse. Även förtäckta hot kan utgöra ett 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.

Nödvärn

Nödvärn

24 kap. 1 § brottsbalken

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

Genom att vara uppmärksam på vad som händer kan du anpassa ditt agerande utifrån situationen och hur den förändras.

Anmäl alla hot

Om hot, våld eller trakasserier förekommer trots förebyggande åtgärder finns det flera saker att göra. Hot ska polisanmälas. Informera säkerhetsansvarig i den egna organisationen eller närmaste chef om det inträffade. Det ger dem de bästa förutsättningarna att fortsätta bygga ett bra skydd. Dokumentera och spara sådant som har anknytning till det misstänkta 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 ansvarar 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 som utgångspunkt Säkerhetspolisens ansvar.

I och med en anmälan kan brottsoffer- och personsäkerhetsarbetet uppgraderas. En anmälan underlättar också underrättelsearbetet. Även om en anmälan inte kan knytas till en gärningsperson 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 du kan göra för att skydda dig själv och dina närmaste. Finns det en hotbild görs en skyddsplan och eventuella säkerhetsåtgärder planeras i dialog med den som hotet riktas mot. Det är Säkerhetspolisen alternativt Polismyndigheten 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 personerna eller för utredningen av sekretess. I vissa fall pågår brottsutredningen parallellt med skyddsarbetet och kan leda till att en gärningsperson identifieras, åtalas och döms. I andra fall går det inte att driva utredningen framåt och förundersökningen läggs ned, men då kan skyddsarbetet ändå fortsätta. Skyddsarbetet beror med andra ord inte på om en gärningsperson har identifierats eller inte, utan utformas efter behovet som finns.

Hot på telefon

- ☐ Lyssna uppmärksamt och avbryt inte den som ringer.
- ☐ Notera tid, bakgrundsljud, kön, ålder, dialekt och liknande.
- ☐ Om möjligt, spela in samtalet.
- ☐ Du kan förlänga samtalet genom att upprepa vad uppringaren säger, låtsas som att det inte går att höra ordentligt och genom att använda fraser som ”Förlåt, jag hörde inte riktigt vad du sa?”. Det kan ge mer information och göra det lättare att identifiera vem som ringde.

6

Säkerhet i vardagen

Säkerhetsåtgärder på plats i hemmet,
för familjen och på arbetsplatsen är viktiga för
att öka säkerheten i vardagen.

För att öka säkerheten i din bostad kan du skaffa ett hemlarm och därmed säkra de vanligaste intrångsvägarna som entrédörrar, fönster som är lätta att nå, stegar som kan användas för att ta sig in 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. Ta hjälp av säkerhetsansvarig i organisationen och i särskilda fall Säkerhetspolisen eller Polismyndigheten. Du kan få råd specifikt om hur det går att förbättra skyddet i bostaden eller på arbetsplatsen och uppmärksamma säkerhetsaspekter i närmiljön.

Dörrar och brevinkast

Bor du i lägenhet är en säkerhetsdörr med extern förstärkt brevlåda det bästa skyddet. Om ytterdörren har ett brevinkast är en förebyggande åtgärd att montera en säkerhetsbrevlåda med brandskydd på insidan av dörren. Istället för brevinkast går det att ha utvändigt låsbar brevlåda eller en postbox.

Se checklista ”Dörrar och brevinkast” sidan 38.

Fönster och glasade ytor

Om det finns glasade partier i eller vid sidan om entrédörren 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. Sidoljusfönster 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. Undvik också att lämna ut nycklar, inpasseringskort och portkoder till exempelvis hantverkare eller städföretag.

Om du tappar bort nycklar, inpasseringskort eller koder 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 avsedda för detta ändamål. Byt därför kod och rengör knappsatsen regelbundet. Nycklar och lås ska vara godkända enligt gällande standard där nycklarna ska vara kopieringsskyddade, helst med behörighetskort. Elektroniska ytterlås ska vara godkända av försäkringsbolaget samt certifierade.

Se checklista ”Nycklar, kort och koder” sidan 38.

Familj – skyddet för närstående

En förövare kan pröva att gå via närstående för att försöka påverka din förmåga att fungera i det politiska uppdraget. Genom medvetna val och råd från säkerhetsansvariga kan ni tillsammans bygga säkerhet. Samtliga familjemedlemmar bör vara införstådda i en eventuell hotsituation och känna till de åtgärder som görs.

Se checklista ”Familj – skyddet för närstående” sidan 38.

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 vilka utrymmen som behöver 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. Undvik 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 att verifiera eventuella obehöriga. De flesta övervakade larm går dessutom att komplettera med rökdetektorer vilket skapar en högre skyddsnivå vid bränder. Ett råd är att sätta upp en skylt om bevakning eller larm vilket kan fungera 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 bland andra larmoperatörer och bevakningsbolag.

SOS Alarm

I nödsituationer går det normalt sett att larma till 112 även om telefonnätet eller sim-kortet inte fungerar. Om du ringer 112 från en telefon utan sim-kort eller som är uppkopplad via mobil roaming den normalt inte har tillgång till visas inte telefonnumret för SOS Alarm.

När du ringer 112 från en mobiltelefon får larmcentralen din position automatiskt via telefonsamtalet. Larmoperatören kommer av säkerhetsskäl alltid be dig att bekräfta din position även muntligen. Via appen ”SOS Alarm 112” kan du vid behov se dina koordinater och läsa upp dem för larmoperatören. Du kan även dela dina koordinater till valfri person via telefonens inbyggda delningsfunktioner. Genom 112-appen får du också viktig information om händelser i din närhet och VMA, viktigt meddelande till allmänheten.

Nödkontakter i mobilen

Vid sjukdom eller olycksfall kan räddnings- och sjukvårdspersonal behöva nå anhöriga eller andra kontakter. Om du har döpt utvalda kontakter i mobiltelefonens adressbok till ICE (In Case of Emergency) kan räddningspersonal snabbt hitta dem om telefonen är upplåst. Du kan själv lägga till nödkontakter som går att nå via en låst mobiltelefon genom att använda inbyggda funktioner i telefonen.

Säkerhet på arbetsplatsen

De flesta reflekterar inte så mycket över de entréer vi passerar eller de lås, koder och inpasseringskort vi använder för att nå fram till arbetsplatsen. Som en förebyggande åtgärd är det klokt att ta reda på vad som gäller kring säkerheten på arbetsplatsen eller partilokalen. Generellt brukar offentliga byggnader och myndigheter 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 i hemmet

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 nås från markplanet har samma skyddsnivå som entrédörrarna.
- ☐ Montera en dörrkik på entrédörren. Då 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, och vid eventuell uppfart och trädgård.

Nycklar, kort och koder

- ☐ Håll bostadsnycklar åtskilda från andra nycklar.
- ☐ Se till att nycklar, kort och koder inte går att identifiera.
- ☐ Byt låscylindrar om nycklar kommit bort.
- ☐ Förvara inte nycklar på platser som är lätta att upptäcka eller där de kan kopplas till en person.
- ☐ Lämna inte nycklar till någon utomstående. Tänk på risken att nycklarna kopieras.
- ☐ Byt lås vid flytt till ny bostad.

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 om någon okänd ringer upp.
- ☐ Be exempelvis servicetekniker, hantverkare eller bud att visa legitimation. Lämna inte okända personer på egen hand i din bostad.
- ☐ Var uppmärksam på okända personer som rör sig utan förklaring i närområdet, 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 personal vid förskola och skola samt ledare inom fritidsaktiviteter informeras. Den som hämtar barnen ska heller inte vara okänd för personalen.
- ☐ Meddela personal om tiderna förändras, till exempel för hämtning.
- ☐ Instruera barnen i hur och när de ska larma 112.

På arbetsplatsen

- ☐ Prata med säkerhetsansvariga i din organisation eller närmaste chef om aktuella säkerhetsåtgärder och vilka säkerhetsrutiner som gäller. Påpeka om du ser brister så att de kan åtgärdas.
- ☐ Se till att det finns en rutin kring hur ni ska hantera oanmälda besökare.
- ☐ Informera berörda medarbetare och säkerhetsansvariga eller partiorganisationen om exempelvis offentliga möten där kontroversiella frågor ska debatteras och det förväntas vara många deltagare så att ni tillsammans har en tanke kring hur ni bemöter hotfulla situationer.
- ☐ Undvik att ta emot okända besökare i enrum. Tror du att mötet kan bli obehagligt eller om 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.
- ☐ Variera färdväg och restider om det finns risk för angrepp.

När hemmet används som arbetsplats

- ☐ Resonera med säkerhetsansvariga i din organisation vilken typ av information du hanterar och hur den ska skyddas vid hemarbete.
- ☐ Använd inte arbetsutrustningen för privat bruk och låna inte ut den till andra.
- ☐ Logga alltid ut så att ingen annan kan komma åt information när du inte använder datorn eller annat uppkopplat arbetsverktyg.
- ☐ Använd endast usb-minnen som är godkända att använda i arbetsdatorn. Privata usb-minnen 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 hålla digitalt, och risken för att andra kan höra eller se vad ni diskuterar.
- ☐ Tänk på vad som visas vid skärmdelning. Undvik att andra tar del av annat än det du avser att dela, 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. Undvik att visa bilder på familjemedlemmar och andra personliga saker.
- ☐ Om andra kan se din skärm, använd ett godkänt skärmskydd på datorn.

➔ **Läs mer** i kapitel 7 ”Säker hantering av teknisk utrustning”.

➔ **Tips**! Läs om säkert distansarbete på Myndigheten för civilt försvars webbplats, mcf.se.

7

Säker hantering av teknisk utrustning

Den tekniska utrustningen vi använder gör oss sårbara för säkerhetshotet från dem som vill skada Sverige. Det är viktigt att hantera både privat teknisk utrustning och den du använder i tjänsten på ett säkert sätt.

När du hanterar säkerhetsskyddsklassificerad information gäller särskilda lagar, förordningar och föreskrifter till skydd för Sveriges säkerhet som du behöver följa. Din egen organisation kan också ha särskilda riktlinjer för tjänstetelefon och annan teknisk utrustning. Råden i det här kapitlet ska ses som en grund.

Tekniska möjligheter förenklar många uppgifter, men innebär samtidigt säkerhetsutmaningar. Trådlösa nätverk (wifi) gör det möjligt för andra att lyssna av nätverkstrafiken och göra intrång utan att ha fysisk tillgång till nätverket. Appar med platspositionering kan användas för att spåra användaren. Intrång och kartläggning kan genomföras av allt från andra stater som vill skaffa sig ett informationsövertag till enskilda personer som är benägna att ta till hot och våld, trakassera eller utföra bedrägerier.

För att minska risken att utsättas behöver du hantera den tekniska utrustningen på ett säkert sätt, såsom mobiltelefoner, datorer och andra uppkopplade enheter. Tänk på att känslig information som inte skyddas kan överhöras eller hamna hos obehöriga. Blanda inte privat teknisk utrustning med den du har fått i tjänsten.

Se över vad teknisk utrustning är döpt till, exempelvis hörlurar, smartklockor, wifi och spårsändare. Det ska aldrig vara något som kopplas till dig själv, såsom ditt namn, adress eller liknande, då det kan underlätta för en person med ont uppsåt att identifiera vem som befinner sig i ett visst område eller utrymme.

Trådlösa nätverk

Mobiltelefoner, surfplattor, aktivitetsarmband, smartklockor och andra uppkopplade enheter är något de flesta använder. Tänk på att publika offentliga trådlösa nätverk, till exempel på hotell, flygplatser, kaféer och bibliotek, medför en ökad risk för avlyssning, intrång och kartläggning. Vid ett intrång kan obehöriga personer få tillgång till både privata uppgifter och uppgifter som rör arbetet, till exempel mejl, personliga kontakter, kalender och rörelsemönster. Ett sådant intrång kan också innebära att funktioner i utrustningen används i den utsattes namn, exempelvis för att skicka mejl eller publicera inlägg i sociala medier.

För att öka säkerheten kan telefonen och innehållet i den förses med särskild kryptering. Men kom ihåg att appar som krypterar meddelanden, exempelvis Signal, Telegram eller WhatsApp, inte får användas för att skicka säkerhetsskyddsklassificerade uppgifter. Mobiltelefoner kan lokaliseras och spåras med hjälp av telefonnumret. Observera att mobiltelefonen kan lokaliseras även om numret är hemligt eller har ett så kallat kontantkortsnummer.

En mobiltelefon och annan uppkopplad teknisk utrustning kan även lokaliseras med hjälp av trådlösa uppkopplingar. Om wifi är påslaget på telefonen söker den aktivt efter nätverk för åtkomst till internet och går därför att lokalisera och spåra. Koppla därför upp dig endast till nätverk som är godkända av din organisation. Om ett sådant trådlöst nätverk inte är tillgängligt är det säkrare att använda uppkoppling via mobilnätet. Var medveten om att all information du skickar eller tar emot via trådlösa nätverk kan läsas av andra om anslutningen inte är säker.

Datorer och teknisk utrustning

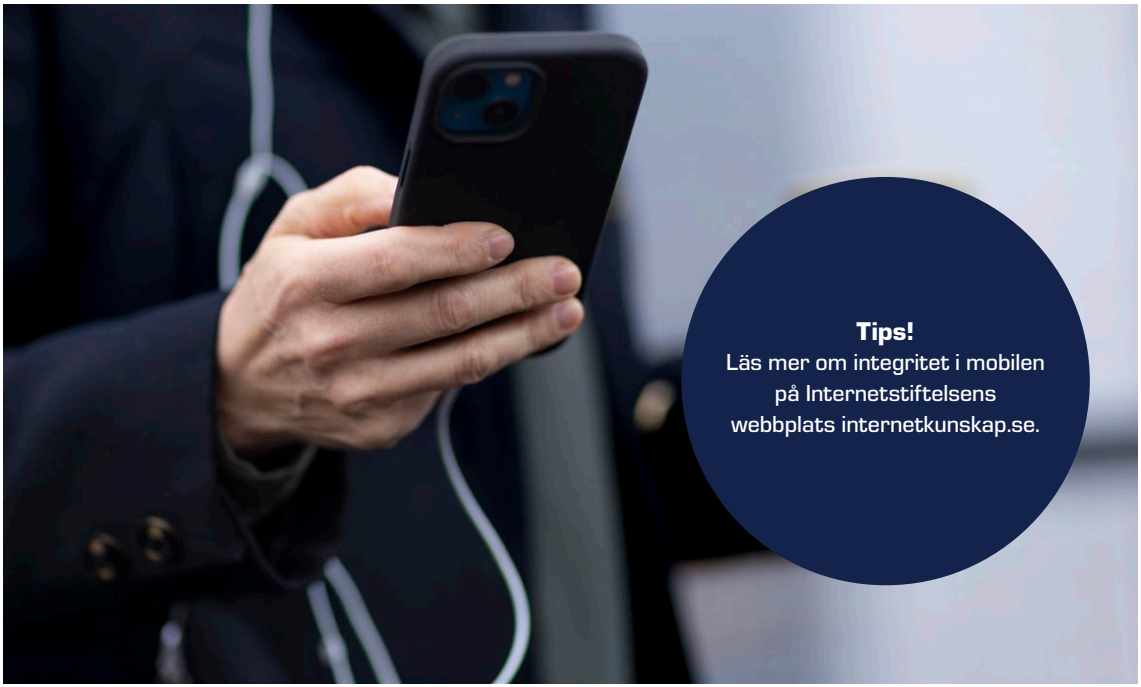
Undvik att använda offentliga datorer eller anslutningar när du hanterar information som inte ska hamna i orätta händer. Använder du någon annans utrustning, till exempel på hotell eller bibliotek, utgå från att någon kan komma över inloggningsuppgifter eller annan känslig information. Tänk på att ta bort filer och program som du laddat ner från webbläsaren. Byt lösenord om du misstänker att det har röjts. Observera att detta bara är en begränsad åtgärd. Det går aldrig att veta hur mycket av aktiviteterna som sparats på en dator någon annan äger. Utgå från att allt sparas. Läs mejl på ett skyddat sätt genom säker inloggning och en krypterad förbindelse, det vill säga genom en vpn-anslutning.

Mobiltelefoner, appar och uppkopplade enheter

Mobiltelefoner och många funktioner och appar i dem förenklar våra liv. Men genom platstjänster blir det samtidigt möjligt att spåra och kartlägga exempelvis en persons träningsrutiner, rörelsemönster, kontakter, var barnen går i skolan, intressen och var någon bor. Att vara medveten om detta kan öka din säkerhet.

När du installerar vissa appar kan de få tillgång till platspositionering. Informationen kan sedan hamna i databaser och säljas vidare. Kom ihåg att även ett aktivitetsband, en smartklocka eller uppkopplade bilar kan avslöja platspositioneringen.

Det finns också appar som automatiskt kontrollerar var mobiltelefoner befinner sig och inkluderar



positionen i exempelvis foton, sökningar, webbsidor och uppdateringar i sociala medier. Om platstjänster är påslaget på bilder följer taggningen med bilderna även när de delas. Se därför över om det är en nödvändig funktion eller om den ska slås av. Ta hjälp av säkerhetsansvariga i organisationen för att ha rätt inställningar.

AI-tjänster

När du använder en AI-tjänst, tänk på vilken information du delar och vem som eventuellt kan få tillgång till den. Dela inte information om dig själv eller andra som du inte vill att AI eller företaget bakom AI-tjänsten ska kunna använda sig av. Dela inte privat information som personnummer, adresser, lösenord och kortuppgifter.

För vissa AI-tjänster sker kommunikationen mellan användare och företagets servrar utan kryptering vilket innebär en risk för att utomstående kan komma åt informationen. När du skriver in information i en AI-tjänst, ställ dig frågan om du skulle vara trygg med att publicera informationen offentligt på internet. Är svaret nej bör du inte heller dela informationen med AI.

Tips! Läs mer om AI-tjänster på Integritetsskyddsmyndighetens webbplats imy.se

Molntjänster

Genom en molntjänst går det att lagra och dela information och material över internet, så att användaren inte behöver lagra material lokalt. Men att spara information i molnet kan innebära att ägaren till informationen förlorar kontrollen över det uppladdade materialet. Sker ett intrång hos företaget som tillhandahåller molntjänsten kan den som gjort intrång potentiellt komma över användares information.

Se checklista ”Lagring i molntjänster” sidan 46.

Risk för avlyssning trots kryptering

Säkerhetsskyddsklassificerad information ska aldrig avhandlas via mobiltelefon eller bärbar teknisk utrustning om de inte har signalskyddssystem godkända av Försvarsmakten.

En av flera åtgärder som kan krävas är att lämna mobiltelefoner utanför rummet när sådan information diskuteras. Tänk även på att andra tekniska enheter med mottagare eller sändare har förutsättningar att skicka vidare uppgifter och ska inte finnas med i rummet. Det gäller till exempel datorer, aktivitetsband, smarta klockor, hörlurar och bilnycklar.

Tips! Läs mer om säkra kryptografiska funktioner på Myndigheten för civilt försvars webbplats mcf.se.

Att använda wifi

- ☐ Anslut aldrig till okända eller publika trådlösa nätverk, eftersom datatrafiken kan övervakas av vem som helst på nätverket. Om ett säkert nätverk inte är tillgängligt är det säkrare att använda uppkoppling via mobilnätet.
- ☐ Om du måste ansluta till ett okänt eller publikt öppet wifi bör det kombineras med så kallad vpn-anslutning. Om egna trådlösa nätverk används, ändra de ursprungliga inställningarna för till exempel namn och lösenord från leverantören. Se även till att aktivera den krypteringsfunktion som ingår för att försvåra avlyssning av datatrafik. Ta hjälp av säkerhetsansvarig om du är osäker.

Datorer och teknisk utrustning

- ☐ Lämna och förvara inte teknisk utrustning utan uppsikt, till exempel i bilar, på hotellrum eller på restauranger.
- ☐ Se till att ingen obehörig kommer åt inloggningsuppgifter till datorer.
- ☐ Notera koder och nummer för att kunna spärra telefonabonnemang om något skulle ske.
- ☐ Stoppa aldrig in okända usb-enheter, minneskort eller annan teknisk utrustning i datorn.
- ☐ Installera, aktivera och uppdatera kontinuerligt antivirusprogram och andra säkerhetsfunktioner.
- ☐ Uppdatera operativsystemet och gör säkerhetsuppdateringar regelbundet. Äldre versioner av teknisk utrustning får inte alltid nya säkerhetsuppdateringar. Byt ut enheten om säkerhetsuppdateringar upphör från leverantören.
- ☐ Använd alltid tvåfaktorsautentisering när det är möjligt. Det ger ett markant ökat skydd jämfört med enbart lösenord.
- ☐ Lösenord ska vara starka och inte gå att gissa sig till. Längden på lösenordet är viktigare än komplexiteten. Ett antal ord som inte har någon koppling till varandra blir en stark lösenfras som ändå är lätt att minnas.
- ☐ Använd aldrig samma lösenord eller lösenfraser för flera användarkonton, vare sig på arbetet eller i privata sammanhang.
- ☐ Använd aldrig jobbets mejladress i privata sammanhang eller för att skapa konton på andra sajter än sådana som är relevanta för arbetet.
- ☐ Nätfiske, så kallad phishing, är något både kriminella och främmande makt ägnar sig åt i syfte att komma över uppgifter och information. Klicka aldrig på länkar i mejlen eller öppna filer från okända avsändare. Ange aldrig personliga koder eller logga in med bank-id efter uppmaning via sms eller mejl. Inga seriösa aktörer skickar sådana uppmaningar.
- ☐ Nyttja inbyggda funktioner i enheten för att kryptera hårddiskar och annan lagringsmedia, exempelvis usb-minne.

➔ **Tips!** På polisen.se kan du läsa om att skydda sig mot bedrägerier.

Lagring i molntjänster

- ☐ Gå regelbundet igenom och uppdatera listan över vilka du delar din information med. Ta bort dem du inte längre vill ska ha tillgång till informationen.
- ☐ Sätt ett starkt och unikt lösenord för att skydda din information. Använd om möjligt tvåfaktors-autentisering.
- ☐ Många molntjänster har inställningar för sekretess och säkerhet. Välj inställningar som ökar säkerheten. Du kan exempelvis se över hur mycket andra ska få veta om ditt konto.

➔ **Tips!** Läs mer om säker användning av molntjänster på Integritetsskyddsmyndighetens webbplats imy.se

Säkrare hantering av mobiltelefonen

- ☐ Uppdatera regelbundet programvaran och appar i mobiltelefonen.
- ☐ Använd pinkod eller ansiktsigenkänning på mobiltelefonen.
- ☐ Håll telefonen under uppsikt. Lämna den inte till någon obehörig eftersom det finns risk för manipulation.
- ☐ Ha inga mobiltelefoner eller annan uppkopplad utrustning med i sammanhang eller rum där säkerhetsskyddsklassificerad information hanteras.
- ☐ I många mobila enheter finns standardinställ-ningar som tillåter trådlös överföring av data. Ta för vana att stänga av trådlös överföring av data som inte används, till exempel Bluetooth, AirDrop eller närfältskommunikation (Near Field Communication, NFC).
- ☐ Acceptera inga oväntade programinstallationer via mejl, sociala medier, sms eller liknande.
- ☐ Använd inga okända minneskort i mobiltelefonen.
- ☐ Om mobiltelefonen innehåller känslig information, överväg att frångå externa leverantörers erbjudande av säkerhetskopiering av innehållet.
- ☐ Kopiera all information till en säker lagringsplats innan mobiltelefonen lämnas in för service eller uppgradering, och gör en så kallad fabriksåterställning.
- ☐ Kolla med organisationens it- eller säkerhets-ansvariga vilka inställningar i mobiltelefonen de rekommenderar.

Appar i mobilen

- ☐ Bedöm om appen är nödvändig att ladda ner eller om den finns som hemsida via en webbläsare i stället. Då ger du inte åtkomst till lika mycket information på din mobiltelefon. Samma gäller för dator och andra smarta enheter.
- ☐ Var restriktiv med att ge appar åtkomst till platsinformation. Aktivera endast om det behövs.
- ☐ Se över integritetsinställningar efter att du uppdaterat operativsystem och appar, då de kan ha ändrats.
- ☐ Ge nya appar som du installerar ett minimum av behörigheter för att de ska fungera.
- ☐ Logga ut från appar när de inte används, annars kan de arbeta i bakgrunden.
- ☐ Radera appar som inte används. Kom ihåg att även radera tillhörande konto.
- ☐ Gå igenom och reglera behörigheterna i apparna regelbundet.

Tips!
Läs mer om informationssäkerhet och säkerhetsskydd på sakerhetspolisen.se.

8

Skydda den personliga integriteten och identiteten

Det kan vara lätt att ta reda på exempelvis personuppgifter och var någon bor. Beroende på situation finns olika åtgärder för att skydda sig. Det kan handla om att minska synlighet och spårbarhet på nätet, att skydda personuppgifter eller i särskilda fall få ett kontaktförbud utfärdat.

I bland är hotbilden sådan att det inte räcker med normala försiktighetsåtgärder, utan det krävs andra säkerhetsåtgärder för att skydda din personliga integritet och identitet.

Skyddade personuppgifter

Uppgifter som registreras i folkbokföringen är som huvudregel offentliga. En utomstående kan alltså med hjälp av uppgifter från folkbokföringen ta reda på uppgifter som i förlängningen används för exempelvis hot eller trakasserier. För att personuppgifter inte ska missbrukas på detta sätt finns åtgärder för 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. Anmälan om behov av skyddad folkbokföring 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.

Tips!
Läs mer om skyddade personuppgifter och sekretessmarkering på skatteverket.se

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 denna, kan komma att lida skada om deras uppgifter lämnas ut. Anmälan om behov av sekretessmarkering görs till Skatteverket. Om en person beviljas sekretessmarkering registrerar Skatteverket den i folkbokföringsdatabasen. Andra myndigheter meddelas markeringen, vilken 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 hot, men det är bra att i förväg vara medveten om hur det kan påverka vardagen. Beroende på om övriga familjemedlemmar också sekretessmarkeras får det olika påverkan. Många myndigheter och andra verksamhetsutövare utser särskilda medarbetare för att hantera kontakter med sekretessmarkerade personer.

En bedömning om hela familjen ska ha sekretessmarkering görs från fall till fall. Även om en sekretessmarkering försvårar kartläggning och spårning, kan den inte helt garantera säkerheten. Bank, post, skola, läkare, föreningar och andra organisationer får inte alltid 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 i sociala medier för att exempelvis sprida falska påståenden. Ha därför kontroll på id-handlingar, var vaksam om någon gör en kreditupplysning och polisanmäl direkt vid misstanke om att du har blivit utsatt för brott. Id-stöldskydd ingår i många hemförsäkringar.

Upplysningstjänster

I Sverige delar många webbplatser med sig av information som finns i folkbokföringen. Det är svårt att helt bli borttagen från den typen av webbplatser med uppgifter om exempelvis adress, telefonnummer, födelsedag eller brotts-register. Om du vänder dig till en sådan webbplats med en begäran om att bli raderad går en del av dem med på att ta bort uppgifterna, medan andra inte gör det. Från vissa går det att bli raderad från den publika sökfunktionen, men uppgifterna är då fortfarande synliga i inloggat läge.

Du kan även kontakta din telefonoperatör och ange att ditt telefonnummer ska vara dolt för nummer-upplysningstjänster. Då kommer numret inte att visas på deras sidor, men de andra uppgifterna kommer även fortsättningsvis att visas.

Kontaktförbud

Syftet med kontaktförbud är att förebygga brott, förföljelse eller andra allvarliga trakasserier. Att överträda ett kontaktförbud är brottsligt och kan leda till fängelse. Kontaktförbudet är tidsbegränsat. Begäran om kontaktförbud kan göras muntligen eller skriftligen till Åklagarmyndigheten eller Polismyndigheten som också kan svara på frågor. Sedan är det åklagare eller domstol som beslutar om kontaktförbud. Det finns fyra olika grader av kontaktförbud:

- **Ordinärt kontaktförbud**, innebär att personen förbudet avser, den så kallade förbudspersonen, inte får besöka, kontakta eller följa efter den skyddade personen.
- **Kontaktförbud avseende gemensam bostad**, innebär att förbudspersonen inte får vistas i en bostad som brukas gemensamt med skyddspersonen.
- **Utvidgat kontaktförbud**, innebär att förbudspersonen inte får besöka eller vara i närheten av skydds-personens bostad, arbetsplats eller andra ställen där hon eller han brukar vara. Det får förenas med villkor om elektronisk övervakning. Om ett kontaktförbud som tidigare utfärdats överträtts ska det utvidgade kontaktförbudet förenas med beslut om elektronisk övervakning.
- **Särskilt utvidgat kontaktförbud**, innebär att förbudspersonen inte får vistas i ett större område runt skyddspersonens bostad, arbetsplats eller andra ställen där hon eller han brukar vara. Detta kan även beslutas som förstahandsåtgärd om det på grund av särskilda omständigheter finns en påtaglig risk för att förbudspersonen kommer att begå brott som innebär ett allvarligt angrepp på skyddspersonens liv, hälsa eller trygghet till person. 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.

9

Avvikande och icke beställda försändelser

Post som skickas till hemmet eller arbetsplatsen kan innehålla obehagliga överraskningar och är något som kan vara svårt att skydda sig emot. En utomstående kan få tag på din adress och skicka brev eller paket med oönskat innehåll.

För att minska risken att få oönskad post till din hemadress kan du använda digital brevlåda och e-faktura när det går. När du beställer varor, välj att få dem levererade till postombud istället för hem. Då har du större kontroll över att du bara får varor du verkligen beställt.

Ett annat sätt är att få en sekretessmarkering hos Skatteverket. Man ska dock komma ihåg att någon som känner till personnumret på den som har sekretessmarkering eller skyddad folkbokföring fortfarande kan skicka post till den personen via Skatteverket.

Läs mer om sekretessmarkering i kapitel 8 ”Skydda den personliga integriteten och identiteten”.

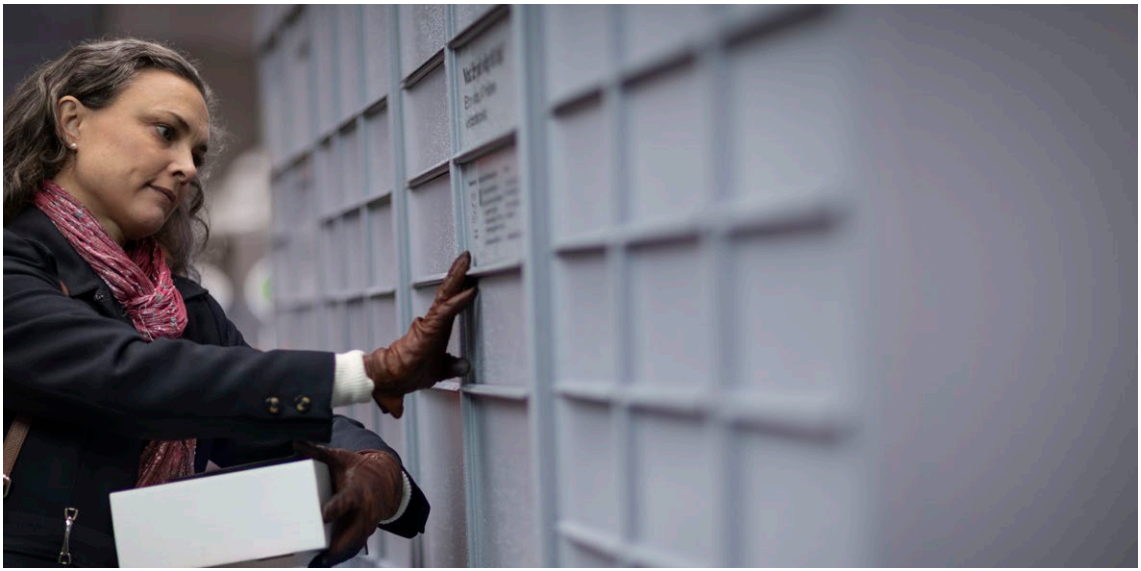
Det är viktigt att vara uppmärksam på icke beställda och avvikande paket och brev, och att hela familjen agerar på samma sätt. Om det finns barn i familjen bör de helst inte öppna post eller paket. Misstänkt farliga försändelser ska alltid polisanmälas.

Misstänkta försändelser

Får du en misstänkt försändelse eller om ett paket ser märkligt ut och har okänd avsändare ska du inte röra eller öppna det, utan kontakta Polismyndigheten. Om möjligt, stäng fönster och dörrar och lämna rummet. Se till att andra inte kommer in. Om du har blivit kontaminerad av något pulver eller ämne, se till att sanera dig omedelbart och undvik närhet till andra människor.

Att hantera hotbrev

Hantera eventuella hotbrev försiktigt och förvara dem skyddat så att polisen kan analysera innehållet och säkra eventuella spår. Undvik därför att andra rör vid hotbrevet, ta i stället ett foto på det. Öppna inte brev i de fall flera försändelser kommer från samma avsändare.



Avvikande försändelser – några kontrollfrågor

- Är försändelsen väntad?
- Hur ser den ut och hur mycket väger den?
- Avger försändelsen ljud eller lukt?
- Hur är adressen och avsändaren skrivna?

Avvikande försändelser

- ☐ Ojämnt eller buckligt utseende.
- ☐ Avvikande vikt, det vill säga ovanligt lätt eller tungt i förhållande till storleken.
- ☐ Mycket tejp eller konstigt emballage.
- ☐ Fettfläckar och läckage av ämne, fast, flytande eller gas.
- ☐ Konstig eller ovanlig lukt.
- ☐ Okänd handskrift.
- ☐ Ovanlig påskrift eller förtryckta bokstäver med text såsom personligt, privat eller brådskande.
- ☐ 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.
- ☐ Plötsliga sjukdomssymptom hos den som öppnat eller hanterat försändelsen.

➔ **Tips!** Läs mer om misstänkta försändelser på Myndigheten för civilt försvars webbplats mcf.se

10

Utpressning, stalkning och rättshaveristiskt beteende

Med ett politiskt uppdrag eller offentligt yrke
följer en risk att bli trakasserad på olika sätt av okända personer.
Det kan exempelvis ske genom telefonsamtal, besök,
brev, mejl eller sociala medier.

Utpressning

Det händer att personer vill störa det demokratiska beslutsfattandet genom utpressning. En utpressare kan använda sig av olika metoder och hot för att tvinga till sig något eller för att påverka beslut. Ibland kan förtäckta insinuationer räcka för att skrämmas. Hållhakar och svagheter kan också utnyttjas. Utpressare kan också ställa krav på att polisen inte ska blandas in. Om en sådan situation uppstår, kontakta säkerhetsansvariga i din organisation och fundera noga på hur kommunikation med Polismyndigheten och andra berörda ska gå till. I dessa situationer är det viktigt att hålla informationen i en så liten krets som möjligt.

Det är bra att ha kontinuerliga samtal med säkerhetsansvariga i din organisation och uppdatera dem om det sker något i privatlivet som skulle kunna utnyttjas av någon med onda avsikter.

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

Stalkning

Olaga förföljelse kallas 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 för den som blir utsatt. Olaga förföljelse är en brottsrubricering som innebär att en gärningsperson begår upprepade brottsliga handlingar, däribland misshandel, olaga tvång, olaga hot, hemfridsbrott eller olaga intrång, ofredande, sexuellt ofredande, skadegörelse eller överträdelse av kontaktförbud.

Om du upplever dig vara förföljd och hotad är det viktigt att anmäla både till säkerhetsansvariga i organisationen och Polismyndigheten. Det är viktigt att det görs en bedömning av den misstänkta personen. Polismyndigheten eller Säkerhetspolisen bedömer om den misstänkta personen är ett hot för din säkerhet eller mot din familj. Därefter görs en bedömning av vilka eventuella skyddsåtgärder som behövs. Detta bör ske i samverkan med säkerhetsansvarig i organisationen. Ett juridiskt biträde eller en motsvarande person kan vara ett stöd och kan även medverka i planeringen av åtgärder.

Personer med rättshaveristiskt beteende

Den som arbetar inom offentlig sektor kan någon gång ha varit i kontakt med en person med ett rättshaveristiskt beteende. Det kan vara svårt att bemöta dessa människor på ett sätt som tillfredsställer deras behov.

Att bli utsatt för en rättshaverist eller annan förföljelse kan leda till att det behöver göras anpassningar på arbetsplatsen för den utsatta personen. I första hand ska du koppla in säkerhetsansvariga i den egna organisationen, men om behov uppstår kontakta Polismyndigheten eller Säkerhetspolisen, beroende på vem som är ansvarig. Bedömning och åtgärder beror på om hotet är personligt riktat eller enbart mot en funktion och arbetsuppgifter, men också hur situationen upplevs. För arbete som kan innebära risk för våld och hot ska det finnas särskilda säkerhetsrutiner.

Hantera stalkning

- ☐ Var tydlig med att du inte vill ha någon kontakt med personen. Undvik därefter all kontakt. Varje kontakt kan innebära en positiv förstärkning och kan öka risken för fortsatt förföljelse, med ökad intensitet.
- ☐ Var uppmärksam på att personen kan göra en digital kartläggning av dig och använda en mängd olika konton och namn för att söka kontakt, exempelvis via mejl eller i sociala medier.
- ☐ Ändra vardagsrutiner genom att gå nya vägar, ändra tider för olika göromål eller välja nya butiker när du handlar. Du kan också behöva byta telefonnummer och mejladress.
- ☐ Se över dina säkerhetsinställningar på sociala medier och andra plattformar.
- ☐ Har du medarbetare som tar emot dina mejl, samtal eller modererar dina sociala mediekonton behöver ni ha en dialog om hur hot ska hanteras.
- ☐ Gör en polisanmälan varje gång du utsätts för något.
- ☐ Berätta om situationen för säkerhetsansvarig i din organisation. Personen kan komma att försöka ta sig in på arbetsplatsen.
- ☐ Dokumentera kontakt eller kontaktförsök från personen, genom att spela in telefonsamtal, skriva upp tidpunkter du blivit förföljd samt när och på vilket sätt du har blivit trakasserad. Spara all information, som exempelvis mejl, sms, samtalslistor i telefonen och alla former av meddelanden som kan styrka hot och trakasserier. Det kan vara viktiga bevis. Berätta för personer i din närhet att du känner dig utsatt.
- ☐ Samarbeta med Polismyndigheten och andra professionella för att få råd kring hur du kan agera. Det går att ansöka om kontaktförbud hos Polismyndigheten.

Hantera rättshaveristiskt beteende

- ☐ Ha en handlingsplan för hur organisationen ska hantera en upprörd, arg eller hotfull person.
- ☐ Det är bra att ha en hög servicenivå, men till en viss gräns i dessa fall.
- ☐ Vid kontakt med en person med rättshaveristiskt beteende – behåll lugnet, höj inte rösten, dras inte med i diskussionen och argumentera inte emot. Var saklig och hänvisa till vad som går att göra, exempelvis 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 en annan person 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 att hänvisa till en annan handläggare eller kollega.
- ☐ Låt personen i fråga få sista ordet, kommentera inte ytterligare.
- ☐ Avsluta eller avbryt samtal som blir kränkande, hotfulla eller meningslösa.

11

In- och utrikes resor

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 du åker.

Det är ovanligt med allvarliga hotsituationer vid resor, men terrorattacker runt om i världen har skapat en större säkerhetsmedvetenhet. Se till att ha en handlingsplan för oförutsedda händelser. 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.

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. Rådgör med säkerhetsansvarig i din organisation innan resan för att bedöma om det är lämpligt att åka och vilka eventuella säkerhetsåtgärder som bör vidtas för att minska riskerna på plats. Det gäller särskilt vid resor till länder som Utrikesdepartementet avråder från.

På Utrikesdepartementets webbplats finns reserekommendationer med råd för olika länder om till exempel säkerhets- och hälsoläget i landet och information om olika krissituationer. Reserekommendationerna finns på regeringen.se/uds-reseinformation. Via appen, ”UD Resklar” kan du ta del av information om resmålet, få råd om du hamnar i en nödsituation utomlands och hitta kontaktuppgifter till Sveriges ambassader. För att ta emot notiser om aktuella händelser eller större kriser i ett specifikt land behöver du aktivera den funktionen i appens inställningar.

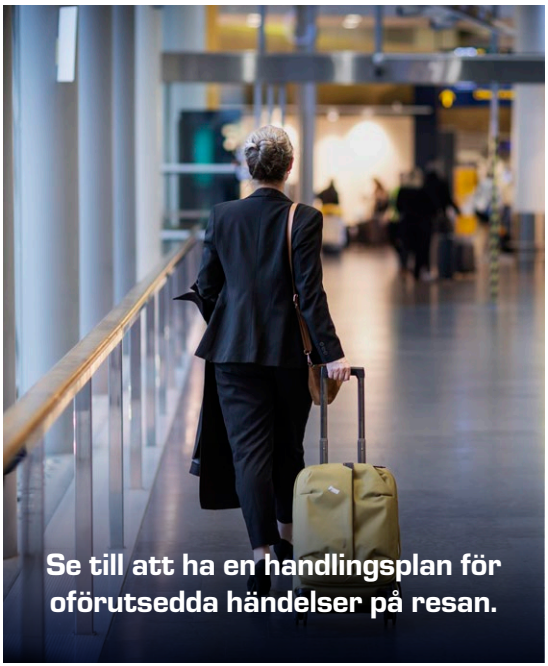
Allvarliga händelser utomlands

Det är ovanligt att svenska medborgare i utlandet utsätts för utpressning eller hamnar i gisslansituationer. Men det kan hända och ställer stora krav på 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 kan du vända dig 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, och 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 aktuella landet och var observant för att upptäcka och undvika tänkbara riskmoment. Var förutseende och ha medicin eller läkemedelsrecept lättillgängliga vid sjukdom. Det kan minska sårbarheten vid hastigt uppkomna situationer. Ha med aktuella telefonnummer till anhöriga, arbetsgivare och försäkringsbolag.

Risker vid flygresor

Vid flygresor är det viktigt att vara uppmärksam på omgivningen och hålla bagaget under noggrann uppsikt. Gå så snart som möjligt innanför säkerhetskontrollen då risken för attentat är högre i vänthallen. Genom att packa rätt undviker du att problem uppstår i säkerhetskontrollen och minskar 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. Ha inte heller någon utvändig märkning med anknytning till ditt uppdrag om det är känsligt, till exempel organisations- eller partiemblem på bagage, kläder, väskor eller liknande.



Se till att ha en handlingsplan för oförutsedda händelser på resan.

Underrättelseinhämtning under utrikesresan

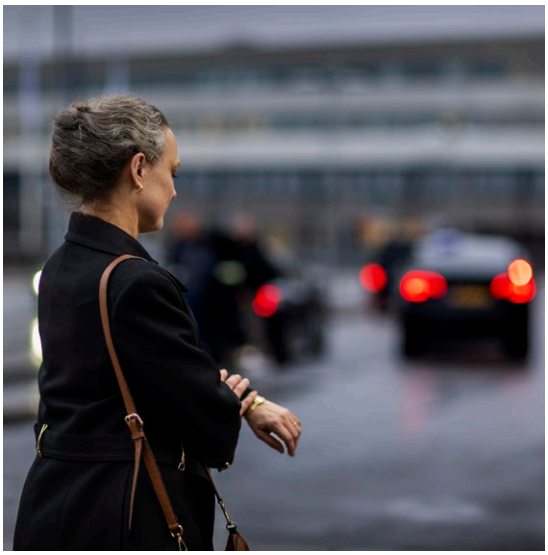
Det finns en potentiell risk att bli kartlagd eller utsatt för underrättelseinhämtning under utrikesresan. Ryssland, Kina och Iran är de länder som utgör det största underrättelsehotet mot Sverige, men det finns även andra länder som har intresse av Sverige. Den som vill kartlägga någon vill komma över 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 du kan vidta för att försvåra för främmande makt. Överväg vilka dokument med säkerhetsskyddsklassificerad information och vilken teknisk utrustning du behöver ta 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 du får 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 du tar en taxi, säkerställ att dörrarna är låsta vid färd. Ta reda på vilka taxibolag som är tillförlitliga. Åk aldrig taxi med någon som har okända medpassagerare. Ha gärna med 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 kontakt på platsen och meddela att ni är på väg, speciellt om resan känns obehaglig. Håll samtalet igång så länge det behövs och fråga chaufförен när ni beräknas vara framme.

Om du använder taxiliknande tjänster bokade via appar, var noga med att kolla att registreringsnumret, bilmodellen och föraren stämmer med informationen i appen. I vissa av dessa tjänsters appar finns en nödhjälpsknapp du kan använda för att ringa efter hjälp. Genom att använda den funktionen får räddningstjänsten tillgång till positionen och information om resan.



Säkerhet på hotellet

Välj ett säkert boende genom att exempelvis höra med kollegor om någon av dem varit på platsen tidigare. Överväg om det är nödvändigt att lämna ut mejladress vid incheckning. En enkel sak som att nämna sitt rumsnummer kan vara av intresse för någon som vill kartlägga dig. Undvik att bo på markplan, eftersom det ökar risken för inbrott. Studera utrymningsplanen för hotellet och ta reda på var de närmaste nödutgångarna finns och om det finns en återsamlingsplats.

Lämna inte känslig och personlig information eller teknisk utrustning på hotellrummet. Betrakta inte hotellets säkerhetsskåp som säkert. Om du måste lämna utrustningen utan uppsikt, använd en så kallad säkerhetspåse för att hantera 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 viktigt att överväga vilken information du lägger ut i sociala medier och vid vilken tidpunkt. Den politiska situationen eller det lokala sammanhanget kan dessutom ha betydelse för hur kommentarer och inlägg uppfattas.

Innan avresa

Informera berörda personer på arbetsplatsen och anhöriga om:

- ☐ Ankomst och återresa.
- ☐ Resmål och kontaktuppgifter. Meddela om det sker förändringar, så att du är nåbar.
- ☐ Hur resan ska ske och vilka aktiviteter och programpunkter som är planerade, särskilt om de är kontroversiella.
- ☐ Vem eller vilka du ska träffa.

Tänk även på att:

- ☐ Res inte ensam om det känns otryggt.
- ☐ Lägg in 112 eller det aktuella landets nödnummer i din mobiltelefon så att du snabbt kan larma.
- ☐ Undvik att dela resedetaljer med okända personer.
- ☐ Ha gärna med en kopia på passhandlingen och extra foton, och förvara dem åtskilda från passet.

Under resor

- ☐ Om du ska byta förbindelser under resan, gör det i lågrisländer.
- ☐ Anländ till resmålet under dagtid eftersom det på kvällar och nätter kan vara svårare att få taxi eller annan hjälp och för att risken för kriminalitet är större.
- ☐ Säkerställ att du kan höra viktig information på flygplatser och få eventuell förvarning vid en incident. Ha därför inte på hörlurar. Samma råd gäller när du färdas med allmänna kommunikationer vid förhöjd terrorhotnivå.
- ☐ Ta bara med nödvändig teknisk utrustning på resan, ha den i handbagaget och lämna den aldrig utan uppsikt.

Vid upphämtning av chaufför

- ☐ Se till att få chaufförens namn och nummer i förväg.
- ☐ Byt telefonnummer med mötande part så att båda kan meddela eventuella förseningar och minimera tiden i ankomsthallen och på parkeringsområdet.
- ☐ Chaufförен kan vara en god källa till information om det aktuella säkerhetsläget.

12

Terrorangrepp och andra attentat

Sannolikheten att drabbas av attentat i form av politiskt eller religiöst våld är liten. Det är ändå viktigt att känna till hur du bör agera om ett angrepp skulle inträffa, vare sig det sker i Sverige eller utomlands.

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 göra stor skillnad eftersom den tid det tar att förstå vad som händer kan vara avgörande för om du hinner ta dig ur situationen.

Var uppmärksam på nödutgångar på ställen där ett dåd kan ske. Ett råd är att inte avfärda oljud som om de vore smällare. En situation som kan uppstå är att någon eller några med onda avsikter tar sig in i ett kommunhus, socialkontor, skola eller andra offentliga byggnader. Rådgör med säkerhetsansvariga i den egna organisationen och se till att ha en handlingsplan för en sådan situation. Den ska innehålla förslag på utrymningsvägar och möjligheter att blockera eller låsa lokaler.

Ta dina iakttagelser på allvar. Ser du något, säg något. Berätta för till exempel personal på plats eller säkerhetsansvariga om något avviker från normalbilden. Larma 112 om något är uppenbart misstänkt.

Vid ett terrorattentat, var sparsam med att använda mobilnätet då alla blåsljusaktörer behöver använda samma nät för att kommunicera och hantera attentatet. Var beredd på att en ny attack kan ske.

När polisen eller i vissa länder militären kommer till platsen, se till att inte misstas för att vara gärningsperson. Håll därför inget i händerna. Lämna inte ett säkert område för att se vad som händer. Följ uppmaningar från polis eller militär samt räddningstjänst.

I händelse av terrorattentat

1. Fly

- ☐ Lämna platsen.
- ☐ Sätt dig i säkerhet.
- ☐ Notera nödutgångar.

2. Sök skydd

- ☐ Sök upp en säker plats.
- ☐ Var uppmärksam.
- ☐ Slå av ljud och vibration på telefonen.
- ☐ Ring inte i onödan till personer i riskområdet.

3. Larma

- ☐ Larma 112 eller landets nödnummer så fort du kan.
- ☐ Berätta om platsen, vad som hänt och om gärningspersonen.

Tips! Läs mer om hur du kan agera vid ett attentat på polisen.se.

Källhänvisning

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

Delar av informationen i boken har inhämtats i samråd med:

- Myndigheten för civilt förvar, mcf.se
- Myndigheten för psykologiskt försvar, mpf.se
- Integritetsskyddsmyndigheten, imy.se
- Internetstiftelsen, internetkunskap.se
- Skatteverket, skatteverket.se
- SOS Alarm, sosalarm.se
- Utrikesdepartementet, regeringen.se/uds-reseinformation

Produktion: Säkerhetspolisen, 2026
Grafisk form: Intellecta
Foto: Säkerhetspolisen
Tryck: Ljungbergs tryckeri
ISBN-nummer: 978-91-86661-29-8
Beställning: Publikationen kan läsas i en onlineversion eller laddas ner på sakerhetspolisen.se, alternativt beställas via sakerhetspolisen@sakerhetspolisen.se.

Läs handboken i mobilen!
På sakerhetspolisen.se/personlig-sakerhet hittar du onlineversionen av handboken ”Personlig säkerhet”.

Säkerhetspolisen är Sveriges nationella säkerhetstjänst och arbetar med att förebygga och avslöja brott mot Sveriges säkerhet, bekämpa terrorism och skydda den centrala statsledningen. Det gör vi för att skydda det demokratiska systemet, medborgarnas fri- och rättigheter och den nationella säkerheten.

Säkerhetspolisen

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

www.sakerhetspolisen.se