Österåker

Österåkers kommuns styrdokument
Datum för antagande:
Diarienummer: KS 2026/0101
Antagen av:
Dokumentansvarig: Avdelning säkerhet, trygghet och civil beredskap

Riktlinjer för att förebygga och hantera otillåten påverkan mot förtroendevalda i Österåkers kommun

POLICY • PROGRAM • STRATEGI • HANDLINGSPLAN • RIKTLINJE

Österåker

Innehåll

1. Inledning

Demokratin vilar på att förtroendevalda kan fatta beslut utan att utsättas för hot, hat, trakasserier eller andra former av otillåten påverkan. Ett angrepp på en enskild förtroendevald är också ett angrepp på den demokratiska processen och ytterst på det samhälleliga förtroende som vår demokrati bygger på.

Österåkers kommun har därför ett gemensamt och grundläggande ansvar att skydda den demokratiska ordningen. Detta innebär att kommunen ska säkerställa en trygg miljö för förtroendevalda, där hot och påverkan förebyggs, upptäcks och hanteras på ett professionellt och rättssäkert sätt. Arbetet ska präglas av transparens, konsekvens och respekt för de demokratiska värderingar som kommunen är satt att försvara.

De nya kraven från 2025 i Kommunallagen att kommuner och regioner måste arbeta förebyggande mot hot och våld mot förtroendevalda ska värna förtroendevaldas trygghet och säkerställa att demokratin kan fungera utan otillbörlig påverkan.

Denna riktlinje beskriver hur kommunen, partierna och förtroendevalda tillsammans ska bidra till att skydda demokratins kärna. Varje enskild förtroendelvald har eget ansvar att hålla sig uppdaterad och följa riktninjerna.

1.1 Syfte

Riktlinjens syfte är att tydliggöra ansvar, organiserande av arbete och ge stöd för att förebygga, upptäcka och hantera otillåten påverkan mot förtroendevalda.

1.2 Målsättning

Målet med riktlinjerna är att säkerställa att alla förtroendevalda kan utföra sitt uppdrag på ett tryggt och säkert sätt. Detta ska uppnås genom att:

- stärka förtroendevaldas trygghet och säkerhet i deras uppdrag.
- minska förekomsten av otillåten påverkan genom ett systematiskt och långsiktigt säkerhetsarbete.
- inträffade incidenter hanteras effektivt, professionellt och med minsta möjliga negativa konsekvens för drabbad förtroendevald.

Målsättningen är också att förtroendevalda och övriga berörda aktörer ska få det stöd och den kunskap som krävs för att kunna bedriva ett förebyggande arbete, samt hantera incidenter på ett sådant sätt att förtroendevalda kan utföra sitt uppdrag under trygga och säkra omständigheter.

1.3 Omfattning

Riktlinjerna omfattar alla former av otillåten påverkan mot förtroendevalda i Österåkers kommun med koppling till det offentliga uppdraget.

Delar av riktlinjen bidrar även med kunskapshöjning vid otillåten påverkan kopplad till partipolitiskt arbete och kan även vara till stöd för otillåten påverkan i privata sammanhang.

2. Ansvar och roller

Österåkers kommun har nolltolerans mot otillåten påverkan riktad mot förtroendevalda samt mot all annan form av brottslig verksamhet. Det är av största vikt att kommunens förtroendevalda ges en trygg och säker arbetsmiljö.

Ansvaret för att skydda och stödja förtroendevalda följer den ordinarie ansvarsfördelningen i kommunen. Det innebär att varje nämnd, styrelse och bolag själv ansvarar för att bedriva ett förebyggande säkerhetsarbete mot otillåten påverkan samt hantera de incidenter som eventuellt uppstår.

2.1 Enskilda politiker

Förtroendevalda har ett ansvar att värna sin egen säkerhet och bidra till att motverka otillåten påverkan inom kommunens demokratiska processer. För att stärka trygghet, integritet och handlingskraft i uppdraget ska följande följas:

- acceptera aldrig otillåten påverkan eller låt beslutsfattandet påverkas av hot, hat, våld eller repressalier.
- genomför kommunens säkerhetsutbildningar, tillämpa riktlinjerna, vidta förebyggande åtgärder samt ta del av tilldelad information om säkerhet för politker på kommunens samlingssida ”Trygg politik” på kommunens webb.
- alltid anmäla alla incidenter till Polis, partiet och kommunen.

2.2 Politiska partier

Respektive parti ansvarar för att stödja sina politikers säkerhet och trygghet vid partirelaterat valarbete och annan partirelaterad verksamhet. Partiet ska bidra både i det förebyggande säkerhetsarbetet och vid incidenter som inträffar i samband med uppdraget.

Partiernas säkerhetsarbete är en viktig del av skyddet för politikerna i det förtroendevalda uppdraget och kompletterar kommunens lagstadgade ansvar enligt 4 kap. 18 a § kommunallagen, där kommunen ska skydda hel- och deltidsarvoderade förtroendevalda från hot och våld.

För att säkerställa ett samordnat och effektivt säkerhetsarbete ska varje parti:

- utse en säkerhetsansvarig kontaktperson som samordnar partiets säkerhetshetsarbete, stödjer politiker och fungerar som kontaktpunkt gentemot kommunen, Polisen och Säkerhetspolisen.
- följa utvecklingen av hotbild mot partiet och dess politiker samt initiera interna bedömningar och åtgärder.
- informera kommunen och Polisen om riskfyllda aktiviteter, samverka inför särskilda aktiviteter och vid allvarliga incidenter.

Kontaktpersonen ska även säkerställa att partiets politiker får del av kommunens utbildningar och rutiner, i linje med kommunallagens krav på att förtroendevalda ska ha nödvändig utbildning för att undvika risker kopplade till hot och våld.

2.3 Ordförande i fullmäktige och nämnder

Ordföranden ansvarar för ordning, trygghet och säkerhet vid sammanträden och har enligt kommunallagen (2017:725), 5 kap. 43§ rätt att visa ut personer – åhörare, ledamöter och ersättare – som efter tillsägelse fortsatt stör sammanträdet. Om ordningen inte kan återställas får ordföranden ajournera eller avsluta mötet.

Inför eller under sammanträden kan ordföranden, enligt lag (2010:294) om säkerhetskontroll vid offentliga sammanträden i kommuner och regioner, besluta om säkerhetskontroll vid inpassering eller i möteslokalen när det finns risk för att brott kan komma att begås som innebär allvarlig fara för liv, hälsa, frihet eller risk för omfattande egendomsskada. Innan ett sådant beslut fattas ska ordföranden samråda med Polismyndigheten och informera kommunen.

Ordföranden ska säkerställa att riskbedömningar görs inför sammanträden med förhöjd risk, att förtroendevalda informeras om säkerhetsåtgärder samt att incidenter rapporteras enligt kommunens rutiner.

Ordföranden ansvarar också för att kommunens riktlinjer är kända och tillämpade av alla ledamöter och att nya förtroendevalda får en introduktion i säkerhetsrutiner och rapportering.

Kommunen stödjer ordföranden att utöva sitt ansvar för ordning, trygghet och säkerhet.

2.4 Kommunen

Kommunen har ett ansvar för de förtroendevaldas säkerhet i samband med utövande av det offentliga uppdraget. Förtroendevalda är dock inte formellt anställda av kommunen. Med anledning av detta är inte otillåten påverkan mot förtroendevalda en arbetsmiljöfråga enligt arbetsmiljölagstiftningen.

Från 1 juli 2025 har kommunen ett förtydligat ansvar att bedriva ett systematiskt säkerhetsarbete med särskilt fokus på förtroendevalda som omfattas av den nya lagstiftningen för heltids- och deltidsarvoderade.

Kommunen ska vidta nödvändiga åtgärder för att förebygga att heltids- och deltidsarvoderade förtroendevalda utsätts för ohälsa eller olycksfall till följd av hot eller våld. Detta följer av 4 kap. 18 a § kommunallagen, vilket innebär att kommunen har ett ansvar för heltids- och deltidsarvoderade förtroendevalda som motsvarar arbetsmiljöansvaret för sina anställda.

För att uppfylla kraven för heltids- och deltidsarvoderade förtroendevalda genomför kommunen:

- regelbundna riskbedömningar
- vidtar relevanta och proportionerliga förebyggande åtgärder
- erbjuder förtroendevalda nödvändig utbildning och tillgängligör information om hur förtroendevalda ska hantera hot- och våldssituationer

2.4.1 Åtgärder för utsatta förtroendevalda

Vid allvarliga eller återkommande incidenter samarbetar kommunen med Polis och beroende på incidenten kan vidta olika former av åtgärder, exempelvis:

- individuella hotbildsbedömningar, personligt anpassade säkerhetsråd, praktiskt stöd vid rättsprocess, krisstöd
- åtgärder i fysisk miljö, möteslokaler, vid resor, bostadsnära åtgärder
- råd om digital exponering, kontosäkerhet

2.4.2 Arbete mot systemhotande aktörer och infiltration

Kommunen ansvarar för att utveckla rutiner, upptäcka, rapportera och motverka påverkan från systemhotande aktörer såsom organiserad brottslighet och extremistiska grupper vilket även ökar säkerheten för förtroendevalda, exempelvis genom att:

- bakgrundskontroller och riskbedömningar i känsliga processer.
- informationsdelning sker med Polis och andra myndigheter.

2.5 Polismyndigheten

Polismyndigheten har en central roll i skyddet av förtroendevalda och i hanteringen av otillåten påverkan. Polisen ansvarar för:

- ta emot och utreda polisanmälningar från förtroendevalda som utsätts för hot, våld, trakasserier eller andra brott som kan kopplas till det offentliga uppdraget.

- genomföra hotbildsbedömningar, särskilt vid återkommande eller allvarliga incidenter, och ge rekommendationer om skyddsåtgärder.
- samverka med kommunen och Säkerhetspolisen i ärenden där det finns för höjd risk eller tecken på systemhotande aktörer eller organiserad påverkan.
- att bistå vid offentliga sammanträden, möten och evenemang när risknivån kräver det, exempelvis genom ökad närvaro eller särskilda säkerhetsåtgärder

Polismyndighetens arbete utgör därmed en viktig del av kommunens helhetsstrategi får att skydda förtroendevalda och upprätthåålla ett tryggt och demokratiskt beslutsfattande.

2.6 Säkerhetspolisen

Säkerhetspolisen har det nationella ansvaret för att skydda demokratin mot aktörer som genom hot, våld, trakasserier, informationsinhämtning eller påverkansoperationer försöker påverka politiska processer eller begränsa det demokratiska beslutsfattandet.

Säpos Handbok Personlig säkerhet (2026) ger politiker och förtroendevalda vägledning om hur de kan minska sin sårbarhet och hantera moderna hot, inklusive digital kartläggning, påverkansförsök, hot från främmande makt, sociala medier, teknisk säkerhet, kampanjarbete och vardagssäkerhet.

Kommunens samverkan med Säpo omfattar:

- etablerade kontaktvägar för säkerhetsrelaterade frågor inom ramen för säkerhetspolisens ansvarar.
- dela relevanta observationer om potentiella hotaktörer.
- att använda Säpos vägledningar i utbildning, riskbedömning och stöd till förtroendevalda.
- involvera Säkerhetspolisen vid allvarliga eller systemhotande incidenter.

3. Ekonomi

Kostnader för förebyggande säkerhetsåtgärder och för hantering av incidenter som rör det offentliga förtroendeuppdraget bekostas av den nämnd, styrelse eller det bolag det förtroendevalda uppdraget avser.

Kostnader som uppstår inom det partipolitiska arbetet ansvarar respektive parti för.

Vid akuta incidenter kan kommunen initiallt hantera vissa kostnader centralt, men beroende på vad som hänt sedan överförs till ansvarig aktör.

4. Rapportering

Rapportering är en förutsättning för att berörda aktörer ska kunna ge stöd, vidta åtgärder och förbättra det förebyggande arbetet.

4.1 Polisanmälan

Kommunen har nolltolerans mot brott, och misstanke om brott ska polisanmälas.

Polisanmälan görs i första hand av den utsatte, detta för att anmälan ska innehålla så korrekt och detaljerad information som möjligt. Både kommunen och politiskt parti kan bistå och stödja den utsatte i samband med polisanmälan som så bedöms behövas.

Vid polisanmälan ska den utsatte ange om den otillåtna påverkan kan ha koppling till det offentliga uppdraget. Straffskärpning kan i sådana fall bli aktuellt.

4.2 Intern rapportering

Förutom polisanmälan ska utsatt anmäla till närmast ansvarig i respektive nämnd, styrelse, bolag och parti samt kommunens säkerhetsavdelning.

Händelser ska registreras i kommunens tillbuds och skaderapporteringssystem.

Rapporterade händelser används för lägesbild, förbättringsåtgärder och internkontroll.

5. Kunskapsunderlag och lägesbild

Brottsförebyggande rådet (Brå) redovisar i Politikernas trygghetsundersökning (PTU) den nationella utvecklingen av förtroendevaldas utsatthet för trakasserier, hot, våld, skadegörelse och andra typer av otillåten påverkan.

Även Sveriges Kommuner och Regioner (SKR), Polismyndigheten och Säkerhetspolisen bidrar med kunskap, metodstöd och analyser som kompletterar Brå:s statistik.

Kommunen har samlat centrala fakta, rutiner och utbildningar för politker och förtroendevaldas trygghet på samlingsplatsen ”Trygg politiker” på kommunens webb.

Otillåten påverkan mot förtroendevalda innebär handlingar som syftar till att påverka politiska beslut, skapa rädsla, begränsa handlingsutrymme eller tysta en politiker. Det kan ske genom hot, trakasserier, våld, skadegörelse, digitala angrepp, otillbörliga erbjudanden eller påverkan mot privatlivet.

Den aktuella nationella lägesbilden visar att 25,4 % av förtroendevalda utsattes för någon form av otillåten påverkan under 2024, där digitala hot är vanligaste formen.

Säkerhetspolisen beskriver dessutom att moderna hot allt oftare riktas via digital kartläggning, tekniska sårbarheter, social manipulation och exponering av privat information.

Kunskap om omfattning och mönster av otillåten påverkan är avgörande för ett effektivt förebyggande arbete. Fakta behövs för att skapa en lokal lägesbild, göra korrekta bedömningar och vidta relevanta åtgärder. Det är därför viktigt att berörda aktörer känner till vilka roller som löper högre risk att utsättas, vilka aktörer som står bakom påverkan, var riskerna är störst och hur ofta händelser förekommer.

5.1 Hur vanligt är otillåten påverkan?

Enligt Politikernas trygghetsundersökning (PTU) 2025 uppgav 25,4 procent av landets förtroendevalda att de utsattes för hot, trakasserier, våld, skadegörelse eller stöld under 2024. Utsattheten är tydligt högre under valår. En majoritet av de utsatta drabbas flera gånger: drygt hälften 2–5 gånger och nära en tredjedel 6 gånger eller fler.

5.1.1 Vilka drabbas mest

Kvinnor är mer utsatta än män: 26,8 % jämfört med 24,4 %.

Riksdagsledamöter har den högsta utsattheten (65 %), följt av regionpolitiker (31 %) och kommunpolitiker (25 %).

Yngre politiker (30–39 år) är mest utsatta (nära 36 %), medan de under 29 år ligger på knappt 30 %.

Utsattheten ökar med graden av offentlig exponering, särskilt i digitala kanaler.

5.1.2 Vem är förövaren

I de flesta fall är förövaren okänd. När en uppfattning finns är det oftast en ensamagerande individ såsom en förargad invånare eller person med rättshaveristiska beteenden. Vanliga motiv är politiskt missnöje, ideologiska skäl eller personlig aggression riktad mot den förtroendevalde.

Säpos handbok beskriver även att förtroendevalda kan bli mål för systemhotande aktörer, exempelvis extremistmiljöer och främmande makt, som kan använda digitala metoder och social manipulation i syfte att påverka politiska beslut.

5.1.3 Var sker utsattheten

Den största delen av utsattheten sker digitalt via sociala medier, e-post och andra digitala plattformar.

Utsatthet sker också vid politiska möten, i offentlig miljö, i anslutning till bostaden och under resor.

Säpos handbok lyfter digital kartläggning, exponering i sociala medier och bristande teknisk säkerhet som centrala riskområden för förtroendevalda.

5.1.4 Vad är det som kan inträffa

Nedan följer områden som kan hjälpa förtroendevalda att känna igen tidiga signaler och agera enligt myndigheters rekommendationer och kommunens rutiner.

Digitala hot och trakasserier:

- hotfulla eller aggressiva meddelanden via sociala medier, e-post eller chatt.
- upprepade kränkande kommentarer eller organiserade hatkampanjer riktade mot förtroendevalda.
- spridning av falska rykten, manipulerade bilder eller vilseledande information som skadar trovärdighet.
- digital kartläggning av personuppgifter, familj, bostad eller dagliga rutiner.
- användning av falska profiler som utger sig för att vara politikern.
- automatiserade bot-konton som förstärker hot, trakasserier eller desinformation, dvs. ett digitalt verktyg som styrs av programvaror.

Fysiska konfrontationer och trakasserier:

- aggressiva eller hotfulla konfrontationer vid politiska möten eller i offentlig miljö.
- personer som följer efter, bevakar eller observerar en förtroendevald i syfte att påverka eller skrämma.
- obehöriga som försöker få tillträde till möteslokaler eller politiska sammanträden för att påverka beslut eller skapa oro.
- fientliga eller störande beteenden i samband med valrörelser, exempelvis vid valstugor, dörrknackning eller offentliga möten.

Otillbörlig påverkan och korruptiva angreppssätt:

- erbjudanden om tjänster, pengar eller andra förmåner i utbyte mot beslut eller ställningstaganden.
- påtryckningar från organisationer, intressegrupper eller individer genom återkommande kontakter i syfte att påverka enskilda politiker.
- försök från närstående, bekanta eller nätverk att påverka politiska beslut.

- aocial manipulation i syfte att få tillgång till intern information, möten, scheman eller andra känsliga uppgifter.

Hot mot privatliv, integritet och närstående:

- hot riktade mot familjemedlemmar, barn eller andra anhöriga.
- doxxing, dvs. spridning av bostadsadress, personuppgifter, bilder eller annan integritetskänslig information.
- hot om att offentliggöra eller sprida privata uppgifter, bilder eller rykten.
- oönskade besök, störande telefonsamtal eller bevakning vid bostaden.
- skadegörelse på bostad, fordon eller annan privat egendom.
- beställning av varor eller tjänster i politikerns namn i syfte att trakassera eller skada.

5.1.5 Konsekvenser för demokratin

Politikernas trygghetsundersökning (PTU) visar att utsattheten påverkar förtroendevaldas möjlighet att fullfölja sina uppdrag.

Många anger att utsattheten leder till förändrat beteende, ökad försiktighet och oro, vilket riskerar att påverka deras beslutsfattande och vilja att fortsätta i sina politiska uppdrag.

Detta medför risker för demokratins representativitet och funktion. Otillåten påverkan mot förtroendevalda är ett mycket allvarligt demokratibrott.

6. Definitioner

Otillåten påverkan:
Samlingsbegrepp för handlingar som syftar till att påverkaförtroendevaldas beslutsfattande med olagliga eller olämpliga medel, exempelvis trakasserier, hot, våld, skadegörelse, utpressning, otillbörliga erbjudanden och andra korruptiva handlingar. Händelsen betraktas som otillåten påverkan om den drabbade uppfattar att syftet var att påverka tjänsteutövningen.

Trakasserier:

Ofredande, förtal, förolämpning, upprepade oönskadekontakter, ryktes-spridning, falska beställningar m.m.

Hot:

Uttalanden eller handlingar som den utsatte uppfattar som allvarliga och som avser att skada person, anhöriga, egendom eller annat av värde.

Hatbrott:

Brott mot någon på grund av hudfärg, nationellt, etniskt ursprung, religion eller sexuell läggning, vilket kan medföra straffskärpning.

Fysiskt våld mot person eller egendom (skadegörelse), inklusive försändelse i syfte att skrämmas eller skada, exempelvis s.k. pulverbrev.

Våld:

Fysiskt våld mot person eller egendom (skadegörelse), inklusive försändelse i syfte att skrämmas eller skada, exempelvis s.k. pulverbrev.

7. Utbildningar och Referenslitteratur

För att säkerställa att alla politiker och förtroendevalda har tillräcklig kunskap och motståndskraft mot otillåten påverkan ska kompetenshöjande insatser löpande berdrivas.

Kommunen samlar relevant fakta, riktlinjer och utbildningar för politiker och förtroendevaldas säkerhet och trygghet på kommunens webbplats -Trygg politiker som är kommunens samligssida med stöd för både det förebyggande arbetet och hanteringen av inträffade incidenter.

Österåkers kommun – samlingssida

- Trygg politiker – kommunens samlingssida för stöd och utbildningar

Sveriges Kommuner och Regioner (SKR)

- SKR – Vägledningar om otillåten påverkan, hot och hat
- SKR- Trygghet för förtroende-valda – stöd, metoder och kunskap för att mot-verka hot och hat

Brottsförebyggande rådet (Brå)

- Brå – Politikernas trygghetsundersökning 2025
- Brå – Handbok: Att förebygga och hantera påverkansförsök (2025)

Regeringen & riksdagen

- Kommunallagen (2017:725)
- Lag (2010:294) om säkerhetskontroll vid offentliga sammanträden i kommuner och regioner | Sveriges riksdag

Säkerhetspolisen

- Säkerhetspolisen – Handbok i personlig säkerhet (digital utgåva 2026)

Arbetsmiljöverket

- Arbetsmiljöverkets föreskrifter och allmänna råd (AFS 2023:2) om planering och organisering av arbetsmiljöarbete – grundläggande skyldigheter för dig med arbetsgivaransvar

Bilaga Checklistor mot otillåten påverkan

Ett första steg i säkerhetsarbetet inför offentliga möten och partirelaterat arbete är att göra en riskanalys, att rådgöra med säkerhetsansvariga om befintliga rutiner, att se över säkerheten och ha beredskap för störningar.

Säkerhetspolisen tillhandahåller i Handbok Personlig säkerhet ett antal checklistor som förtroendevalda och andra berörda bör ta del av och helt eller delvis tillämpa i olika sammanhang. Checklistorna är generellt utformade och alla detaljer inte alltid tillämpliga i alla sammanhang.

Österåker kommuns riktlinjer innehåller några av Säkerhetspolisens checklistor. Alla checklistor finns i Säkerhetspolisen Handbok Personlig säkerhet, som är tillgänglig på kommunens samlingssida ”Trygg Politiker”.

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.

Österåker

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.

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.

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?

Österåker

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.

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.

Österåker

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.

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.