nimblr

Säkerhetsmedvetenhet i offentlig sektor 2027

# Från krav till beteende

Praktisk vägledning för dig som ansvarar för IT eller informationssäkerhet i en kommun, region eller myndighet.

30 september 2026

**Fem minuter. Fem frågor.**

Vad behöver vi ha på plats? Hur når vi olika roller? Vad ska vi följa upp? Hur mycket administration kräver det? Vad behöver vi tänka på inför inköp eller upphandling?

# Det här behöver IT och informationssäkerhet veta

Från 1 oktober 2026 gäller MCFFS 2026:11. Föreskrifterna är en del av ett mer systematiskt och riskbaserat cybersäkerhetsarbete. För IT och informationssäkerhet blir tre delar särskilt viktiga när det gäller medarbetarnas säkerhetsmedvetenhet:

**Anpassa efter roll.** Alla i organisationen möter inte samma risker. De allmänna råden anger att utbildning och övning bör anpassas efter medarbetarens roll, ansvarsområden och befogenheter.

**Träna och öva över tid.** Verksamheten ska fastställa vilka informationsinsatser, utbildningar och övningar som personalen ska genomföra före och under anställning eller uppdrag. Regelverket anger ingen bestämd frekvens, men arbetet behöver vara planerat och fungera över tid.

**Följ utvecklingen över tid.** De allmänna råden rekommenderar en utbildningsplan som beskriver både när och hur aktiviteter ska genomföras, följas upp och utvärderas.

Utmaningen är därför inte bara att erbjuda utbildning. Det är att få träning och övning att fungera för olika roller i hela organisationen, följa utvecklingen och göra det utan att skapa onödig administration.

## 1. Kraven i praktiken

**Det här är krav:** Verksamheten ska fastställa vilka utbildningar, övningar och informationsinsatser personalen ska genomföra före och under anställning eller uppdrag.

**Det här rekommenderas i de allmänna råden:** Utbildning och övning för egen personal bör anpassas efter roll, ansvarsområden och befogenheter. Verksamheten bör också ha en utbildningsplan som beskriver när och hur aktiviteterna ska genomföras samt när och hur de ska följas upp och utvärderas.

Regelverket anger däremot inte hur ofta medarbetarna ska utbildas eller tränas, eller vilken plattform eller leverantör som ska användas.

## 2. Läget i offentlig sektor

Den senaste Cybersäkerhetskollen visar att många offentliga organisationer fortfarande har en bit kvar i det systematiska cybersäkerhetsarbetet. Över 300 organisationer inom offentlig förvaltning deltog i mätningen 2025, och resultaten visar stora skillnader både mellan organisationer och mellan olika delar av säkerhetsarbetet.

Det är viktigt i sammanhanget. De nya kraven handlar inte om att lägga till ytterligare en kurs, utan om att få utbildning och övning att fungera som en del av ett större, systematiskt arbete.

För IT och informationssäkerhet blir nästa fråga praktisk: **Hur får vi det att fungera för alla de olika människor och roller som finns i organisationen?**

## 3. Det ska fungera för hela organisationen

I en kommun, region eller myndighet finns många olika roller med olika arbetsuppgifter, behörigheter och risker. En ekonom, en HR-medarbetare, en IT-administratör eller en medarbetare inom vård och omsorg möter inte samma situationer.

Därför behöver träningen vara relevant för den roll och de risker medarbetaren faktiskt möter. Det betyder inte att varje roll behöver ett helt eget utbildningsprogram, men vissa delar behöver anpassas.

| Roll eller grupp | Exempel på situationer att träna på |
|---|---|
| **Ekonomi** | Falska fakturor, ändrade betalningsuppgifter och brådskande betalningsförfrågningar |
| **HR och lön** | Ändrade löneuppgifter, personuppgifter, bilagor och förfrågningar som ser ut att komma från en medarbetare eller chef |
| **IT och helpdesk** | Kontoåterställning, behörigheter, phishing mot privilegierade konton och falska supportärenden |
| **Ledning** | Riktade angrepp, falska förfrågningar i chefers namn och situationer där tidspress eller beslutsmandat utnyttjas |

### Alla arbetar inte på samma sätt

Rollanpassning handlar inte bara om innehållet. Träningen behöver också fungera för olika sätt att arbeta. En medarbetare inom vård och omsorg, teknisk verksamhet eller fältarbete har andra förutsättningar än någon som arbetar framför en dator hela dagen.

Korta moment och format som är enkla att komma åt gör det lättare att nå fler delar av organisationen, till exempel träning som fungerar i mobil, surfplatta och dator, utan separat inloggning.

**Har ni redan en lärplattform eller annan säkerhetsutbildning?** Den behöver inte ersättas. Titta i stället på vad ni redan täcker och vad som saknas. Kan ni anpassa träningen efter roll? Öva med realistiska angrepp? Följa hur medarbetarna agerar över tid? Det är där ni ser vilka delar som behöver kompletteras.

## 4. Från genomförd kurs till beteendeförändring

En genomförd kurs visar att medarbetaren har tagit del av utbildningen. Men för IT och informationssäkerhet är det också relevant att veta hur medarbetarna agerar när de möter ett misstänkt meddelande eller en simulerad attack.

Genom att kombinera genomförande med beteendedata går det att följa både om träningen når fram och hur säkerhetsbeteendet utvecklas över tid.

| Mått | Vad det kan visa |
|---|---|
| **Slutförandegrad** | Om den planerade utbildningen når målgruppen |
| **Klick eller inlämnade uppgifter** | Hur medarbetarna agerar i simuleringar |
| **Rapporteringsgrad** | Hur stor andel som rapporterar misstänkta meddelanden |
| **Tid till rapportering** | Hur snabbt IT får kännedom om ett misstänkt meddelande |
| **Upprepade riskbeteenden** | Om samma individer eller grupper återkommande behöver ytterligare stöd |

**Följ utvecklingen över tid.** Ett enskilt resultat säger inte särskilt mycket, eftersom simuleringar bland annat varierar i svårighetsgrad. Följ därför hur klick, rapportering och andra beteenden förändras över flera simuleringar.

**Rapportering är minst lika intressant som klick.** En minskande klickfrekvens visar en del av utvecklingen. En ökande rapporteringsgrad och kortare tid till rapportering visar en annan.

## 5. Hur mycket arbete ska IT behöva lägga?

Säkerhetsträning ska fungera över tid utan att IT behöver administrera varje aktivitet manuellt. Därför är det värt att titta på arbetsinsatsen redan när ni utvärderar ett upplägg eller en lösning.

| Återkommande moment | Fråga att ställa | Målbild |
|---|---|---|
| **Användare** | Kan användarhanteringen synkas med organisationens användarkatalog (t ex Entra ID)? | Slippa underhålla användarlistor manuellt |
| **Roller och grupper** | Kan träning tilldelas utifrån roll eller grupp? | Rätt träning till rätt personer |
| **Träning och simuleringar** | Kan återkommande aktiviteter planeras och schemaläggas? | Kontinuitet utan manuella utskick |
| **Påminnelser** | Kan påminnelser automatiseras? | Slippa jaga genomförande manuellt |
| **Uppföljning** | Kan resultat och utveckling följas direkt i lösningen? | Automatiserade och standardiserade rapporter. |

**En rytm som håller över tid.** Regelverket anger ingen bestämd frekvens för utbildning och övning. Det viktiga är därför att hitta en rytm som fungerar för organisationen och dess riskbild. Nya medarbetare behöver komma in i arbetet, kunskapen behöver hållas aktuell och övningar behöver återkomma och varieras. På så sätt blir säkerhetsmedvetenhet ett löpande arbete, snarare än en enskild utbildningsinsats.

## 6. Så kan Nimblr stödja arbetet

Nimblr kompletterar organisationens befintliga utbildningar med återkommande träning, realistiska simuleringar och uppföljning av säkerhetsbeteenden. Programmet är byggt för att kunna pågå löpande utan att IT behöver planera och administrera varje enskild aktivitet.

| Behov | Så stödjer Nimblr |
|---|---|
| **Träna hela organisationen** | Korta utbildningsmoment som återkommer över tid. Kursen öppnas direkt från mejlet, utan separat inloggning, och fungerar i mobil, surfplatta och dator. |
| **Anpassa efter roll** | Rollbaserad träning för bland annat ekonomi, HR, IT, DevOps och ledning. |
| **Öva på verkliga situationer** | Phishing- och smishing-simuleringar där användaren får direkt återkoppling efter interaktion. |
| **Minska administrationen** | Utbildningar, simuleringar och påminnelser skickas automatiskt, och rapporterna tas fram automatiskt. IT behöver inte planera varje aktivitet. |
| **Följa säkerhetsbeteendet** | Genomförd träning och resultat från simuleringar kan följas över tid. |
| **Följa rapportering** | IT kan följa hur misstänkta meddelanden rapporteras, inte bara hur många som klickar. |

### Från träning till beteendeförändring

Nimblr kombinerar utbildning, övning och uppföljning i ett löpande program:

**Träna → Öva → Ge direkt återkoppling → Följ utvecklingen → Fortsätt träna**

Medarbetarna får korta utbildningsmoment och möter sedan realistiska phishing- och smishing-simuleringar. När någon interagerar med en simulering ges direkt återkoppling, så att lärandet sker nära själva situationen. Resultaten ger IT möjlighet att följa hur beteendet utvecklas över tid och var ytterligare träning kan behövas.

### Vad ser vi i Nimblrs data?

Vi har analyserat 4,8 miljoner simulerade phishingmejl som skickats till nästan 200 000 medarbetare i svensk offentlig sektor mellan januari 2025 och september 2026. Tre resultat är särskilt intressanta inför 2027.

## 4 gånger

högre klickfrekvens på mejl som ser ut att komma från den egna organisationen jämfört med mejl från externa avsändare. En falsk medarbetarenkät hade särskilt hög klickfrekvens, 16,9% klickade.

**→ För er 2027: Öva på mejl som liknar dem medarbetarna faktiskt får, exempelvis från HR, ledningen, kollegor och de verktyg ni använder varje dag.**

## 2,6 gånger

högre klickfrekvens när samma mejl är skrivet på svenska i stället för engelska.

**→ För er 2027: Träna på svenska och med svenska exempel. Felfri svenska är inget tecken på att ett mejl är äkta.**

## 40 %

färre klick efter ett år med återkommande säkerhetsträning.

**→ För er 2027: Ta reda på var ni står i dag och följ utvecklingen över tid. En egen utgångspunkt gör det lättare att sätta mål och se hur beteendet förändras.**

| Resultat | Vad det visar | För er 2027 |
|---|---|---|
| **Interna mejl jämfört med externa** | Fyra gånger högre klickfrekvens på mejl som ser ut att komma från den egna organisationen. | Öva på mejl från HR, ledning och kollegor samt meddelanden från verktyg som används i det dagliga arbetet. |
| **Svenska jämfört med engelska** | 2,6 gånger högre klickfrekvens när samma mejl är skrivet på svenska. | Träna på svenska och med svenska exempel. Felfri svenska är inget tecken på att ett mejl är äkta. |
| **Förändring i klick över tid** | 40 % färre klick efter ett år med återkommande träning. Tre av fyra organisationer hade lägre klickfrekvens än vid starten. | Ta reda på var ni står i dag, sätt mål och följ utvecklingen över tid. |

### Rapportering är nästa steg

Klickfrekvensen visar bara en del av bilden. Gör det enkelt för medarbetarna att rapportera misstänkta mejl och följ hur rapporteringen utvecklas över tid, inte bara antalet klick. Varje rapport kan ge IT en tidig signal om ett möjligt angrepp. Rapporteringen är också ett mått på hur väl säkerhetsträningen fungerar. Att låta bli att klicka på ett misstänkt mejl är ett första steg. Att rapportera det är nästa steg: medarbetaren känner igen hotet och agerar för att skydda organisationen.

## Vad säger de som använder Nimblr?

För att säkerhetsträning ska fungera över tid behöver den vara relevant för medarbetarna och enkel att administrera och följa upp.

**18 av 19** administratörer i svensk offentlig sektor gav Nimblr betyget 8 eller högre på en tiogradig skala. Undersökningen omfattar 16 organisationer.

**94 %** av svaren i Nimblrs relevansmätning anger att utbildningarna är relevanta eller mycket relevanta. Resultatet bygger på över 350,000 svar från Nimblrs användare.

Så beskriver två administratörer sina erfarenheter:

> **”Återkopplingen vi får från våra deltagare handlar om relevans, korthet och ibland hur roliga kurserna är.”**
>
> IT-specialist, större kommun

> **”Korta utbildningar som medarbetarna tar sig tid att göra. Uppföljningen för oss administratörer är väldigt lättillgänglig.”**
>
> Chef, större myndighet

## Hur gör andra i offentlig sektor?

Nimblr används redan av kommuner, myndigheter och andra offentliga verksamheter i Sverige.

# 7. Inför val eller upphandling av en lösning

Utgå från vad organisationen behöver kunna göra, vilka grupper som ska omfattas, hur arbetet ska följas upp och hur mycket administration lösningen kräver. Då blir det lättare att jämföra olika alternativ på samma grund.

Cybersäkerhetslagen påverkar också offentlig upphandling. Krav på informations- och cybersäkerhet kan behöva ställas på leverantörer, även när leverantören inte själv direkt omfattas av regelverket.

### 13 frågor att ställa leverantören

1. Hur anpassas innehåll och övningar efter roll och risk?
2. Hur fungerar lösningen för medarbetare som inte sitter framför en dator hela dagen?
3. Vilka beteenden kan vi följa och hur kan resultaten analyseras över tid?
4. Hur styrs behörigheten på individ-, grupp- och organisationsnivå?
5. Hur varieras simuleringar i tema, kanal och svårighetsgrad?
6. Hur läggs användare till och tas bort? Kan det synkas automatiskt?
7. Vilka delar av programmet är automatiserade och vilka kräver manuellt arbete?
8. Vilket underlag finns för uppföljning och rapportering?
9. Var lagras data och hur hanteras personuppgifter?
10. Hur fungerar lösningen tillsammans med vår befintliga IT- och utbildningsmiljö?
11. Hur ser införande, support och löpande förvaltning ut, och vilken intern arbetsinsats krävs?
12. Kan vi tala med en offentlig organisation av liknande storlek eller verksamhet?
13. Genom vilka partners, avtal eller andra inköpsvägar kan lösningen köpas?

#### Hur kan Nimblr köpas?

För offentlig sektor är inköpsvägen en viktig del av valet av lösning. Nimblr kan köpas direkt eller genom någon av våra samarbetspartners. Vi arbetar med IT-partners och återförsäljare över hela Sverige, så det finns ofta en väg som passar de avtal ni redan har.

Osäkra på vilken väg som passar er? Kontakta oss, så hjälper vi er hitta rätt inköpsväg och sätter er i kontakt med rätt partner.

## 8. Arbetslista för 2027

Använd listan för att se vad som redan finns på plats och var ni behöver komplettera.

- [ ] Vi har identifierat vilka grupper och roller som behöver utbildning och övning utifrån vår riskbild.
- [ ] Vi har en plan för när och hur utbildning, övning och informationsinsatser ska genomföras, följas upp och utvärderas.
- [ ] Nyanställda och nya uppdragstagare omfattas av relevanta aktiviteter.
- [ ] Träningen fungerar för olika roller och arbetsdagar, även för medarbetare som inte arbetar framför en dator hela dagen.
- [ ] Vi följer både genomförande och relevanta beteenden, till exempel klick, rapportering och utveckling över tid.
- [ ] Vi har bestämt hur resultat får användas och vem som har tillgång till information på individ-, grupp- och organisationsnivå.
- [ ] Vi kan följa utvecklingen utan omfattande manuell sammanställning.

- [ ] Vi vet vad våra befintliga utbildningar och lärplattformar redan täcker och var det finns luckor.
- [ ] Vi har definierat våra krav på bland annat informationssäkerhet, personuppgiftshantering, datalagring och integrationer.
- [ ] Vi har undersökt hur lösningen kan köpas genom våra befintliga inköpsvägar och avtal.
- [ ] Vi har möjlighet att tala med en jämförbar offentlig organisation före beslut.

### Var börjar vi?

Tre frågor räcker för att komma vidare:

**Vilka roller och beteenden är viktigast för oss att påverka?**

**Vad kan vi följa upp idag, och vad saknar vi?**

**Vilka återkommande moment behöver automatiseras för att arbetet ska fungera över tid?**

## Kontakta Nimblr

### Vill ni se hur Nimblr kan fungera hos er?

Vi visar gärna hur Nimblr kan användas för återkommande träning, simuleringar och uppföljning i en offentlig verksamhet. Vi kan också, när det är möjligt och godkänt av kunden, hjälpa er att komma i kontakt med en offentlig organisation som redan använder Nimblr.

**Kontakta oss och boka en genomgång**

### Källor


MCFFS 2026:11, föreskrifter och allmänna råd om säkerhetsåtgärder och ledningens utbildning, Försvarets radioanstalt (FRA).

Cybersäkerhetslag (2025:1506), i kraft sedan 15 januari 2026.

Myndigheten för civilt försvar, Fortsatt allvarliga brister i Sveriges cybersäkerhetsarbete, 2 mars 2026.

Upphandlingsmyndigheten, Cybersäkerhetslagens (NIS2) påverkan på offentlig upphandling, 19 januari 2026.