

Basic Security

Kurs



2
0
2
5

Dette kurset er utviklet for å gi virksomheten din et tydelig konkurransefortrinn innen sikkerhet. I samarbeid med ledende eksperter fra **Advansia** og **Lørn**, kombinerer vi solid bransjekunnskap med praktiske verktøy som kan tas i bruk umiddelbart.

Med innsikt fra **Stig Brekke**, **Eli Westad Garmann**, **Miriam Søetorp**, **Jack Fischer Eriksen** og **Frode Skaarnes**, er programmet skreddersydd for å styrke organisasjonens kompetanse og skape målbare resultater.



Frode Skaarnes



Eli Westad Garmann



Stig Brekke



Miriam Søetorp



Jack Fischer Eriksen

Basic Security



Formål

Dette kurset bygger bevissthet og motstandskraft mot komplekse trusler som retter seg mot digitale, fysiske og menneskelige sårbarheter. Kurset vil gi medarbeidere og ledere praktiske verktøy for å gjenkjenne trusler, redusere sårbarheter og styrke organisasjonens sikkerhetskultur.

Kurset tilbys i to tilpassede versjoner for å møte ulike roller i organisasjonen, og de 12 modulene kan spres utover et helt år.

Avansert løp gir ledere og spesialister dypere innsikt og strategiske verktøy for å integrere sikkerhet i både policyer og kultur.

Grunnleggende løp gir alle ansatte praktisk kunnskap og gode vaner som gjør det mulig å beskytte seg selv, sine kollegaer og organisasjonen i det daglige arbeidet.



Estimert tid til fullføring:

Avansert løp – 5 timer

Grunnleggende løp – 80 minutter

Fullstendig kursmoduloversikt:

1. Sikkerhetskultur
2. Påvirkning
3. Digital sosial manipulering
4. Fysisk sosial manipulering
5. Sårbarheter
6. Ubevisste innsidere
7. Bevisste innsidere
8. Trusselvurdering
9. Verdivurdering
10. Risikovurdering
11. Cybersikkerhet
12. Reisesikkerhet

Basic Security



Modul 1: Sikkerhetskultur

Kort beskrivelse

Utforsker hvordan felles verdier, holdninger og atferd danner ryggraden i organisasjonens sikkerhetssystem, og hvorfor både ledelse- og medarbeiderengasjement er avgjørende.

Læringsmål

Avansert løp

- Analysere hvordan verdier, normer og holdninger påvirker organisasjonens sikkerhet.
- Identifisere lederansvar i utvikling og opprettholdelse av sikkerhetskultur.
- Utvikle kommunikasjonsstrategier som fremmer tillit og åpenhet.
- Vurdere og implementere mekanismer for kontinuerlig forbedring av sikkerheten.

Grunnleggende løp

- Forstå hvorfor sikkerhetskultur er viktig for alle.
- Gjenkjenne egen rolle i hverdagslige sikkerhetsrutiner.
- Lære enkle steg for å bidra til en tryggere arbeidsplass.

Forventede utbytter

Avansert løp: Evne til å integrere sikkerhet i organisasjonskultur og policyer.

Grunnleggende løp: Bevissthet om personlig ansvar og bidrag til helhetlig sikkerhet.

Basic Security



Modul 2: Påvirkning

Kort beskrivelse

Ser på hvordan interne og eksterne aktører forsøker å påvirke oss, fra utenlandske desinformasjonskampanjer til dagligdagse overtalesesteknikker.

Læringsmål

Avansert løp

- Identifisere statlige og ikke-statlige påvirkningsstrategier i digitale og sosiale sammenhenger.
- Forklare Cialdinis seks universelle påvirkningsprinsipper og deres sikkerhetsmessige konsekvenser.
- Vurdere sårbarheter i organisasjonen for manipulasjonskampanjer.
- Bygge motstandskraft hos seg selv og sine team.

Grunnleggende løp

- Kjenne igjen vanlige påvirknings- og manipulasjonsteknikker.
- Lære å faktasjekke og praktisere kritisk tenkning.
- Forstå viktigheten av å motstå feilinformasjon.

Forventede utbytter

Avansert løp: Verktøy for å trene ansatte og beskytte organisasjonens tillit.

Grunnleggende løp: Bevissthet om daglige påvirkningstaktikker og hvordan stå imot dem.

Basic Security



Modul 3: Digital sosial manipulering

Kort beskrivelse

Dekker hvordan cyberkriminelle bruker frykt, tillit og fristelser til å lure enkeltpersoner til å gi fra seg informasjon eller tilgang.

Læringsmål

Avansert løp

- Beskrive digitale sosialmanipulasjonsmetoder (phishing, smishing, vishing, spear-phishing).
- Analysere eksempler på avanserte angrep (f.eks. deepfake-basert svindel).
- Utvikle forebyggende policyer, opplæring og rapporteringsrutiner.
- Vurdere hvordan organisasjonskultur påvirker motstandskraft mot manipulering.

Grunnleggende løp

- Gjenkjenne digitale svindelforsøk og mistenkelige meldinger.
- Lære trygge rutiner for passord, lenker og autentisering.
- Vite hvordan og når man skal rapportere hendelser.

Forventede utbytter

Avansert løp: Evne til å implementere organisatoriske forsvarstiltak og bevisstgjøringstrening.

Grunnleggende løp: Trygghet i å oppdage og unngå svindel i arbeidshverdagen.

Basic Security



Modul 4: Fysisk sosial manipulering

Kort beskrivelse

Ser på manipulasjon i ansikt-til-ansikt situasjoner, inkludert spionasje, svindel og bedrag i personlige og profesjonelle sammenhenger.

Læringsmål

Avansert løp

- Analysere eksempler på fysisk manipulasjon og infiltrasjon.
- Identifisere menneskelige sårbarheter som utnyttes i fysiske møter.
- Utarbeide strategier for å styrke fysisk sikkerhet og personellsikkerhet.
- Vurdere organisatoriske rutiner for å oppdage og redusere risiko.

Grunnleggende løp

- Forstå hvordan fysisk sosial manipulering arter seg.
- Lære å stille spørsmål ved uvanlige forespørsler og adferd.
- Vite hvordan man skal eskalere eller rapportere mistenkelige kontakter.

Forventede utbytter

Avansert løp: Bedre evne til å oppdage og håndtere innsiderisiko eller ekstern infiltrasjon.

Grunnleggende løp: Økt personlig bevissthet og praktiske tiltak i daglige møter.

Basic Security



Modul 5: Sårbarheter

Kort beskrivelse

Hvordan sårbarheter ser ut på tvers av mennesker, teknologi, bygninger og organisasjonen - og hvordan de kan reduseres gjennom opplæring, tydelige policyer og kontinuerlig forbedring. Dekker menneskelige (stress, lav bevissthet, kognitive skjevheter, sosial manipulering), fysiske (bygg, strøm, kjøling, brann), digitale og organisatoriske svakheter.

Læringsmål

Avansert løp

- Identifisere menneskelige sårbarheter og foreslå tiltak.
- Vurdere fysiske svakheter i kritisk infrastruktur.
- Forklare organisatoriske hull og foreslå styringstiltak.
- Prioritere forbedringer med risikobasert og oppdatert tilnærming.

Grunnleggende løp

- Gjenkjenne de mest vanlige menneskelige og fysiske faresignalene.
- Anvende noen få høyeffektive tiltak (opplæring, adgangskontroll, klare ansvarsforhold).

Forventede utbytter

Avansert løp: Evne til å kartlegge sårbarheter på tvers av mennesker/teknologi/fasiliteter/organisasjon og anbefale prioriterte tiltak.

Grunnleggende løp: Bevissthet om vanlige fallgruver og evne til å følge enkle rutiner som reduserer risiko i hverdagen.

Basic Security



Modul 6: Ubevisste innsidere

Kort beskrivelse

Innsiderisiko som omfatter personer som utilsiktet lekker informasjon eller blir manipulert til «uforsiktig deling» av informasjon. Modulen viser hvordan kultur og bevissthet kan redusere denne risikoen, med eksempler som Olly Robbins og DNV-saken.

Læringsmål

Avansert løp

- Definere innsidertyper og trusselaktører (stat og organisert kriminalitet) og forklare hvorfor innsidere er så verdifulle.
- Gjenkjenne mønstre for påvirkning og tidlig rekruttering samt vanlige personlige risikofaktorer.
- Styrke en «just culture» med rapportering og støtte for høyrisikopersonell.
- Øve på sikre informasjonsdelingsvaner både på og utenfor jobb.

Grunnleggende løp

- Kjenne igjen vanlige delings- og manipulasjonstaktikker og rapportere tidlig.
- Følge enkle grunnregler for samtaler, sosiale medier og reiser.

Forventede utbytter

Avansert løp: Evne til å veilede team i å oppdage innsidertegn og gjennomføre enkle innsiderisikovurderinger.

Grunnleggende løp: Trygghet i å gjenkjenne og raskt rapportere mistenkelig tilnærming.

Basic Security



Modul 7: Bevisste innsidere

Kort beskrivelse

Tre kategorier - rekrutterte, selvmotiverte og profesjonelle innsidere - med reelle eksempler (DNV, Melita Norwood, Eirik Jensen) og praktiske forebyggingstiltak.

Læringsmål

Avansert løp

- Skille mellom motivasjon og metoder hos rekrutterte, selvmotiverte og profesjonelle innsidere.
- Analysere klassiske rekrutterings- og kultiveringsmønstre og langtids samarbeid i det skjulte.
- Implementere kontrolltiltak: rollebasert oppfølging, sårbarhetssamtaler og etablere en kultur hvor de som har "krysset grensen", forteller dette til sin leder.
- Forstå aktivistdrevne lekkasjer og kulturelle mottiltak.

Grunnleggende løp

- Kjenne igjen tegn på rekruttering og selvmotiverte innsidere.
- Vite når og hvordan bekymringer om kollegaer eller prosesser skal rapporteres.

Forventede utbytter

Avansert løp: Evne til å vurdere innsiderscenarioer og anvende balanserte, personellsikkerhetsmessige mottiltak.

Grunnleggende løp: Evne til å varsle tidlig og bidra til en trygg rapporteringskultur.

Basic Security



Modul 8: Trusselvurdering

Kort beskrivelse

Hvordan identifisere trusselaktører, sannsynlighet og konsekvens - og prioritere tiltak. Inkluderer aktuelle eksempler (terrorisme og ekstremisme) og enkel veiledning under akutte hendelser.

Læringsmål

Avansert løp

- Beskrive hovedkategorier av trusler (stat, spionasje, sabotasje, terrorisme, organisert kriminalitet, aktivisme) og deres mål/metoder.
- Vurdere om organisasjonen er et plausibelt mål og hvorfor.
- Oversette trusselinnsikt til konkrete sikkerhetstiltak og øvelser.

Grunnleggende løp

- Kjenne igjen hovedtrekkene i trusselbildet og enkle beskyttelsestiltak.
- Huske enkel veiledning under akutte hendelser (f.eks. «løp/gjem deg»).

Forventede utbytter

Avansert løp: En dokumentert trusselvurdering med prioriterte tiltak og øvingsplaner.

Grunnleggende løp: Bevissthet om hvem som kan være en trussel og hva man bør gjøre dersom de prøver.

Basic Security



Modul 9: Verdivurdering

Kort beskrivelse

Hvordan identifisere og klassifisere hva som er mest verdifullt - informasjon og fysiske eiendeler - og dokumentere dette som grunnlag for risikovurdering og beslutninger om beskyttelse. Inkluderer kvalitative/kvantitative metoder og vurdering av konfidensialitet, integritet og tilgjengelighet.

Læringsmål

Avansert løp

- Skille mellom kvalitative og kvantitative vurderinger og vite når de brukes.
- Klassifisere informasjon/objekter etter konfidensialitet, integritet og tilgjengelighet.
- Planlegge og gjennomføre en avgrenset vurdering (mål, omfang, verdier).
- Dokumentere prosess, deltakere, funn og resultater tydelig.

Grunnleggende løp

- Gjenkjenne hvilke informasjonstyper/objekter som er «kritiske» og hvorfor.
- Bruke en enkel klassifisering og dokumentere den konsekvent.

Forventede utbytter

Avansert løp: Et forsvarbart register over verdier med klassifiseringer som styrer kontroll og tilganger.

Grunnleggende løp: En enkel, brukervennlig liste over nøkkelverdier og deres betydning.

Basic Security



Modul 10: Risikovurdering

Kort beskrivelse

Hvorfor, når og hvordan gjennomføre sikkerhetsrisikovurderinger - både som prosess og som produkt som støtter beslutninger og prioriteringer.

Læringsmål

Avansert løp

- Forklare drivere for risikovurderinger (lovkrav, hendelser, press fra interessenter) og hvordan resultatene brukes av beslutningstakere.
- Involvere riktige interessenter og ledelse i de riktige fasene.
- Utføre trinnvise metoder tilpasset konteksten; presentere resultater via matrise eller kvalitativ beskrivelse.
- Planlegge risikohåndtering og oppfølging; oppdatere i takt med endringer i trusler og verdier.

Grunnleggende løp

- Beskrive sannsynlighet/konsekvens på et grunnleggende nivå.
- Vite hva som bør eskaleres og hvordan valgte tiltak følges opp.

Forventede utbytter

Avansert løp: En repeterbar vurdering med tydelig risikobilde, diskusjon om risikovilje og prioriterte tiltak.

Grunnleggende løp: Evne til å bidra med innspill og forstå oppsummering av risiko.

Basic Security



Modul 11: Cybersikkerhet

Kort beskrivelse

De mest effektive virksomhetstiltakene (NSMs «topp fem») og daglige rutiner for enkeltpersoner (sterke unike passord + MFA, oppdateringer, phishing-bevissthet, unngå åpne Wi-Fi-nettverk).

Læringsmål

Avansert løp

- Forklare og implementere de fem mest effektive virksomhetstiltakene (patching, administratorrettigheter, autentisering, modernisering, programvare-hvitlisting).
- Kvantifisere hvordan disse reduserer vanlige skadevare- og passordangrep.
- Oversette policy til daglig praksis i team (oppdateringer, MFA, programvaregodkjenning).

Grunnleggende løp

- Praktisere de «fire store» personlig: unike passord + MFA, oppdatere alt, tenke før du klikker, unngå åpne Wi-Fi-nett.
- Vite når personell fra IT/sikkerhet skal kontaktes.

Forventede utbytter

Avansert løp: Et praktisk cybergrunnlag som kan stoppe de fleste standardangrep.

Grunnleggende løp: Sikrere daglige vaner som reduserer personlig risiko betydelig.

Basic Security



Modul 12: Reisesikkerhet

Kort beskrivelse

Praktisk veiledning for trygg reise i tre faser - før, under og etter - med fokus både på personlig sikkerhet og beskyttelse av enheter/informasjon.

Læringsmål

Avansert løp

- Forberede reiseplaner og beredskap; minimere eksponering av mennesker og data før avreise.
- Anvende sikre rutiner under reisen (hotell, transport, møter og digital hygiene).
- Avslutte reisen sikkert (sjekk av enheter, datahåndtering, rapportering).

Grunnleggende løp

- Følge en enkel sjekklister for personlig og informasjonsmessig sikkerhet på reise.
- Vite hva som bør rapporteres dersom noe føles uvanlig.

Forventede utbytter

Avansert løp: En gjenbrukbar mal for reisesikkerhet og briefing.

Grunnleggende løp: Trygghet til å reise smartere og beskytte det du har med deg.

Basic Security

Kurs



Pris eks mva



Avansert: 990 NOK/lisens

Grunnleggende: 490 NOK /lisens

Ta kontakt for pakkepris:

contact@lorn.tech

+47 91687688