Myndigheten för samhällsskydd och beredskap

Texter i webbutbildningen ”Digital informationssäkerhetsutbildning för alla (Disa)”

Disa

Digital informationssäkerhetsutbildning för alla

Vi lever idag i ett informationssamhälle där information bearbetas, lagras och kommuniceras i större omfattning än tidigare. Både på vår arbetsplats och i vårt privatliv hanterar vi dagligen stora mängder information. Vet du hur du hanterar informationen säkert? Vet du vilka rutiner som gäller på din arbetsplats? Vet du till vem du rapporterar incidenter?

Välkommen till MSB:s grundutbildning i informationssäkerhet!

Om MSB:s arbete med informationssäkerhet

Myndigheten för samhällsskydd och beredskap (MSB) har i uppgift att samordna arbetet med samhällets informationssäkerhet. Arbetet berör hela samhället – från organisationer, kommuner, andra myndigheter och företag, till enskilda individer. MSB:s uppdrag är att stödja förebyggande åtgärder och arbeta med att främja ett systematiskt långsiktigt arbete med informationssäkerhet på alla nivåer i samhället.

MSB tar kontinuerligt fram föreskrifter, vägledningar och stöd till hjälp för informationssäkerhetsarbetet i samhället. Du finner dessa på webbplatsen www.informationssäkerhet.se.

Om Disa

Disa består av tio avsnitt. Genom animerad film introduceras i varje avsnitt ett grundläggande koncept inom informationssäkerhetsområdet. För att du ska kunna tillgodogöra dig utbildningens innehåll på ett så bra sätt som möjligt bör du aktivt arbeta med vår checklista under hela utbildningen. Spara ner pdf:en så kan du enkelt fylla i den under utbildningens gång.

I checklistan fyller du i vad som gäller för just din organisation. När hela checklistan är ifylld kan du använda den vid behov i ditt dagliga informationssäkerhetsarbete. Checklistan kan också användas som ett intyg på att du gått kursen.

Tips!

Checklistan kan användas som diskussionsunderlag. Om ni saknar rutiner eller regler för informationssäkerhet i din verksamhet kan Disa hjälpa er att komma igång.

Varför är informationssäkerhet så viktigt?

Fördjupande text

Alla organisationer är beroende av information för att kunna utföra sina uppdrag. Vi kan kommunicera, lagra, förädla och till och med styra processer med information. Vår information är värdefull, både för organisationer och för den enskilda individen. Ibland är informationen livsviktig om den återfinns i patientjournaler eller i styrsystem i kärnkraftverk. Går den informationen förlorad eller är felaktig kan det få katastrofala följder.

Vi behöver därför skydda vår information så att den alltid finns när vi behöver den, att vi kan lita på att den inte är manipulerad och att endast behöriga personer får ta del av den. Med informationssäkerhet menar vi därför möjligheten att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet hos våra informationstillgångar.

01 Säkert beteende

Ingress

Du hanterar information varje dag. Ett säkert beteende på arbetsplatsen minskar riskerna för att din information förvanskas, förstörs eller försvinner. Hur mycket tänker du på informationssäkerhet i din vardag?

Film: Säkert beteende

Du hanterar information varje dag. Från det att du vaknar till dess att du går och lägger dig på kvällen. Information du hanterar som är privat får du själv ansvara för. Tillhör informationen din arbetsgivare behöver du ta reda på hur du ska hantera den så att du inte utsätter din organisation för risker

Tänker du på vem som kan se över axeln på dig när du kollar din jobbmail på morgonen eller när du jobbar från ett café och på tåget? Tänker du på vem som kan höra när du pratar i telefon i hissen upp till kontoret? Vad har du framme på skrivbordet? Låser du din datorskärm när du hämtar en kopp kaffe? Eftersom det är i ditt dagliga arbete som den viktigaste informationssäkerheten skapas så är det viktigt att du tänker säkert. En oavsiktlig handling kan lätt få onödigt stora konsekvenser. Med ett säkert beteende minskar risken.

Interaktiv fråga

En kollega ringer dig på mobiltelefonen när du sitter på bussen på vägen hem. Du känner att det kanske inte är ett lämpligt samtalsämne i en offentlig miljö. Vad gör du?

- ✓ Förklarar att du just nu inte kan prata om detta över telefon och ber att få återkomma.
- o Talar så tyst du kan. Det gäller ju att klara av jobbet så du kan släppa det när du kommer hem.

- Lägger på luren utan att säga någonting. Det gäller att tydligt visa att det inte är okej att prata om sånt utanför jobbet.

Hur gör din organisation?

Ta reda på vad som gäller i din organisation.

Vad hittar du din organisations riktlinjer för informationssäkerhet?

Hur gör din organisation? Fyll i checklistan!

02 Lösenord

Ingress

Lösenord skyddar din information på nätet men kan vara svåra att komma ihåg. Hur väljer du dina lösenord? Använder du samma lösenord hemma som du gör på jobbet?

Film: Lösenord

Användarnamn och lösenord identifierar oss på nätet i system, tjänster och applikationer. Undvik därför alltför enkla lösenord eller lösenord som kan kopplas till dig som person. Använd heller inte samma lösenord för olika konton. Skriv inte ner dina lösenord där andra kan komma åt dem.

Ett lösenord blir säkrare ju längre och mer oförutsägbart det är. Men långa lösenord kan vara svåra att komma ihåg. En nonsensramsa är lätt att minnas för dig, men svårare för hackaren att knäcka. Tips! Istället för att behöva minnas många och långa lösenord kan du ta hjälp av en lösenordshanterare.

Interaktiv fråga

Varför bör du inte ge ditt lösenord till någon annan?

- Det finns risk att de som inte är vana vid dina lösenord skriver fel och därmed blir spärrade.
- Om lösenordet används av olika personer finns risk att det spärras av de automatiska larmsystemen.
- ✓ Om andra använder din inloggning kan du bli ansvarig för något de råkar göra på datorn.

Hur gör din organisation?

Ta reda på vad som gäller i din organisation.

Vilka riktlinjer gäller för lösenord i din organisation?

Hur gör din organisation? Fyll i checklistan!

03 Säkerhetskopiering

Ingress

Alla känner vi någon som förlorat viktig information på grund av att datorn kraschat. Säkerhetskopiering är nödvändigt när du jobbar digitalt. Var sparar du dina filer?

Film: Säkerhetskopiering

Saker kan hända med din information. Din dator kan krascha och du kan råka tappa mobila enheter. Du eller någon tjänst du använder kan bli hackad. Bränder, strömavbrott och översvämningar kan göra informationen svår eller omöjlig att komma åt.

Säkerhetskopiering måste göras för att du ska kunna återställa ditt material om datorn eller datafilerna försvinner. Hemma får du sköta detta själv. Men på din arbetsplats finns ofta rutiner för säkerhetskopiering. Spara hellre en gång för mycket så du slipper göra om ditt arbete.

Fördjupande text

Varför är säkerhetskopiering så viktigt?

Säkerhetskopiering av filer och system görs för att du ska kunna återställa material om datorn går sönder eller om datafilerna skadas på annat sätt. Det kan handla om allt från dataintrång till brand. Beroende på din arbetsplats policy så görs säkerhetskopiering olika ofta.

Om du råkar radera eller skriva över ett dokument, kontakta din it-support så kan de hjälpa dig att återställa materialet. I arbetslivet har din arbetsgivare oftast färdiga rutiner för säkerhetskopiering, vilken information som säkerhetskopieras, hur ofta säkerhetskopiering sker, och var säkerhetskopiorna sparas. Kontrollera vilka rutiner som gäller för din arbetsplats.

I privatlivet är säkerhetskopiering ofta minst lika viktigt. Många kan vittna om värdefull information som de förlorat i diskkrascher. Det handlar om allt från viktiga examensuppgifter i skolan till bilder på barn eller släkt.

Det finns flera tjänster, inte minst molntjänster, och funktioner som förenklar säkerhetskopiering. Ta reda på vilken lösning som passar bäst för dig, men tänk på att inte sammanblanda privat och jobbrelaterad information.

Interaktiv fråga

Vad av följande är viktigt att tänka på när det gäller säkerhetskopiering?

- ✓ Förvara alltid dina säkerhetskopior på ett säkert ställe.
- o Det viktigaste med backup är att det faktiskt sker. Hur uppgifterna sedan hanteras är däremot inte så noga.

- Säkerhetskopiering är bara viktigt om din verksamhet hanterar stora finansiella transaktioner eller om det finns särskilda arkivregler för den.

Hur gör din organisation?

Ta reda på vad som gäller i din organisation.

Vilka rutiner gäller för säkerhetskopiering på din arbetsplats?

Hur gör din organisation? Fyll i checklistan!

04 Molntjänster

Ingress

Det är vanligt att man använder molntjänster på arbetsplatsen. Vet du vilken information du får lagra i molnet?

Film: Molntjänster

Molntjänster är ett smidigt verktyg för dig och din organisation att använda i arbetet. Molntjänster underlättar lagring och delning av information och används ofta vid säkerhetskopiering.

Använd bara molntjänster som din organisation tillåter och bara för den information som tjänsten är godkänd för. Blanda inte privat information och företagsinformation. Var noga med att använda separata konton och starka lösenord.

Tänk på att lagring av information hos en tredje part såsom en molntjänst kan innebära att du utsätter din information för risker. Du blir beroende av att nätverksuppkopplingen fungerar och det finns risk att informationen läcker, förändras eller förstörs utan att du kan påverka. Regler för molntjänster bör finnas i din organisation.

Fördjupande text

Molntjänster

Det finns idag flera molntjänster som vi använder dagligen, inte minst för att dela filer och lagra information. Molntjänster är sådana tjänster som nås via internet och som ger möjlighet till resursdelning, snabb skalbarhet och självbetjäning. Den som levererar en molntjänst har ofta en standardiserad miljö där alla kunder samsas om utrymmet på hårdvaruplattformar som befinner sig i stora datorhallar. Ett vanligt sätt att betala för molntjänster är utifrån antalet timmar processorerna använts, mängden minne och nätverkstrafik, och antalet konton.

För medarbetare i offentlig sektor gäller det att tänka på vilken information som kommuniceras till och från molntjänsten och hur den behandlas där. För information med särskilda hanteringsregler, såsom information som bedöms omfattas av sekretess och personuppgifter, måste organisationen göra en samlad bedömning om informationen får

hanteras i molntjänster och i så fall vilka. Det gäller på samma sätt för hantering av annan känslig information så som företagshemligheter.

Det finns flera risker med att hantera information i molntjänster. De som tillhandahåller molntjänsten kan ta del av innehållet, tillgången till informationen kan bli lidande om tjänsteleverantören får problem och du blir beroende av att kommunikationsvägen till molntjänsten (nätverket) fungerar. Varje organisation bör noga överväga hur information används och lagras i molnet.

Interaktiv fråga

Varför bör du tänka dig för innan du använder molntjänster för fildelning eller säkerhetskopiering?

- o Molntjänster har ibland svårighet med att hantera vissa filformat, till exempel PDF.
- o Lagring i molnet innebär i vissa fall att svenska tecken (ääö etcetera) förvanskas.
- ✓ I många fall innebär lagring i molnet att du inte vet var eller med vilken säkerhet informationen hanteras.

Hur gör din organisation?

Ta reda på vad som gäller i din organisation.

Vilka regler finns för molntjänster i din organisation?
Vilka molntjänster använder ni?

Hur gör din organisation? Fyll i checklistan!

05 E-post

Ingress

Vi kommunicerar dagligen med e-post både privat och på jobbet. Vet du vilken information du får skicka via din jobbmejl?

Film: E-post

E-post kan liknas vid ett vykort. Det finns inget kuvert som hindrar den som vill från att läsa informationen. Beroende på vem som äger den tjänst du använder för e-post kan informationen resa över landsgränser och lagras i serverhallar i länder med annan lagstiftning än i ditt land. Mejla därför ingenting du inte vill att andra ska läsa. Många organisationer har regler för hur du får använda din jobbmejl, vad du får skicka för information och om du får använda jobbmejlen för privata ändamål.

Interaktiv fråga

Vad är sant när det gäller möjligheten att skicka känsliga uppgifter med e-post?

- ✓ Betrakta en vanlig e-post som ett vykort. Du har inga garantier för att inte andra läser den.
- o Har du ordning på dina inloggningsuppgifter är det ingen fara att skicka känsliga uppgifter.
- o Om du har uppdaterat ditt virusskydd är det ingen fara att skicka känsliga uppgifter via din vanliga e-post.

Hur gör din organisation?

Ta reda på vad som gäller i din organisation.

Vilka regler gäller för din jobbmejl?
Får du använda den privat?

Hur gör din organisation? Fyll i checklistan!

06 Sociala medier

Ingress

Sociala medier är ett bra sätt att nå ut med information och används både av organisationer och av privatpersoner. Men vad behöver du tänka på när det gäller sociala medier?

Film: Sociala medier

Idag använder sig de allra flesta av sociala medier. Många använder sociala medier privat men både näringslivet och offentlig sektor använder sig av sociala medier för kommunikation och marknadsföring. En värld där alla är på sociala medier ger många nya möjligheter, men kan också medföra risker.

Gränsen mellan vad som är ditt privata användande av sociala medier och vad du gör i jobbet kan lätt suddas ut. Det är viktigt att du tänker på när och hur du uttalar dig som representant för din organisation och när du använder sociala medier som privatperson. Tänk på vilken information du lägger ut och vem som får tillgång till den. Inlägg sprider sig snabbt till en större krets än du hade tänkt dig och är svåra eller omöjliga att radera.

Interaktiv fråga

Vad behöver du tänka på om du har konton och är aktiv på sociala medier?

- o Jag behöver inte tänka på någonting.
- ✓ Jag tänker efter före eftersom allt jag lägger upp kan spridas till en större krets än menat och att det är svårt att radera om jag ångrar mig.
- o Sociala medier är bara en rolig gren, ingen tar det på allvar ändå.

Hur gör din organisation?

Ta reda på vad som gäller i din organisation.

Har ni riktlinjer på arbetsplatsen för hur du får använda sociala medier?

Hur gör din organisation? Fyll i checklistan!

07 Granska avsändaren

Ingress

Det blir allt svårare att avgöra om den information du får kommer från en trovärdig avsändare. Vad har du för strategier för att undvika att råka ut för bedrägerier på nätet?

Film: Granska avsändaren

Det har blivit allt vanligare med it-relaterade brott. Det ställer högre krav på oss att vi granskar avsändaren. Social manipulering, eller social engineering som är den engelska termen, utnyttjar sociala relationer och öppen information om dig i syfte att få tillgång till hemlig eller känslig information. Genom e-post, telefon eller via sms kan du luras att uppge information eftersom du uppfattar avsändaren som trovärdig. En persons röst och ansikte kan till och med manipuleras och användas för att få dig att lämna ut information om din organisation och om dig själv. Det är vanligt att it-relaterade brott vill påskina att det är bråttom och att du måste åtgärda något på en gång. Bedöm först relevansen i meddelandet. Varför har just du fått det? Är det trovärdigt? Vem är avsändaren? Skicka aldrig finansiell eller personlig information utan att först ha verifierat avsändaren.

Om du är osäker, kontakta avsändaren personligen eller via ett listat telefonnummer. Om du har råkat uppge känslig information om din organisation, rapportera det genast.

Interaktiv fråga

Du har fått ett mejl från en gammal kollega som tipsar dig om en jätteintressant artikel. Du får känslan av att något inte riktigt står rätt till men du kan inte sätta fingret på varför du känner så. Vad gör du?

- o Klickar på länken. Du minns kollegan som ordentlig och pålitlig så det är ingen fara.
- ✓ Du ringer organisationens växelnummer och ber att bli kopplad till din gamla kollega för att dubbelkolla innan du öppnar länken.
- o Du raderar mejlet omedelbart. Du har hört att man inte ska klicka på länkar så du litar inte på något.

Hur gör din organisation?

Ta reda på vad som gäller i din organisation.

Om du råkat uppge känslig information om dig eller din organisation, vem rapporterar du det till?

Hur gör din organisation? Fyll i checklistan!

08 Skadlig kod

Ingress

Idag pratar man ofta om virus, trojaner och maskar. Vet du vad det är och hur du kan skydda dig mot det?

Film: Skadlig kod

Det blir allt vanligare med trojaner, maskar och andra typer av skadlig kod som kan angripa din dator för att användas som en väg in i organisationens system. Du riskerar att drabbas av skadlig kod när du använder okända USB-minnen, öppnar bilagor i e-posten eller klickar på länkar. Bedrägerier som nätfiske (så kallad phishing) vill få dig att göra just det eller uppge bank- och personuppgifter. Ransomware, eller utpressningsvirus, blockerar tillgängligheten till dina filer med kryptering.

Du riskerar också att drabbas av skadlig kod om du råkar surfa in på en infekterad sida eller klickar på en annons. För att förhindra pop-up fönster och oönskade annonser kan du använda dig av en annonsblockerare som filtrerar bort oönskad reklam. Det är viktigt att du installerar nya säkerhetsuppdateringar omedelbart och att du har ett antivirusprogram. Om du misstänker skadlig kod eller tror att du klickat på en olämplig länk eller bilaga bör du rapportera det genast.

Fördjupande text

Vad är skadlig kod?

Skadlig kod är ett samlingsbegrepp för det man i dagligt tal kallar virus, så som trojaner och maskar. Traditionellt sett riskerar man att drabbas av skadlig kod när man öppnar okända bilagor i e-posten, surfar på internet eller importerar filer till sin dator via olika media.

För att undvika virusangrepp är det viktigt att du håller din dator uppdaterad med de säkerhetsuppdateringar som din leverantör skickar ut. Du bör även överväga att skaffa ett antivirusprogram, ett program som är gjort särskilt för att söka efter och ta bort filer som är infekterade av virus.

Så snart du märker att du drabbats bör du lämna datorn till din it-support. Om du drabbats är det viktigt att du ändrar alla dina lösenord.

Undvik riskerna på nätet genom ett säkert beteende. Vanligtvis räcker det med att du frågar dig själv hur du skulle agera i verkligheten och sedan agera på liknande sätt i den digitala världen. Ge inte ut mer information än nödvändigt om dig själv, klicka inte på länkar som du inte vet vad de innehåller och kommunicera som grundregel bara med personer som du känner eller vet vilka de är.

Om du har fått ett mejl som du är tveksam till, ring och hör efter med personen eller organisationen som du tror har skickat det om avsändaren stämmer. Mejlbedrägerier som nätfiske (phishing) har blivit alltmer vanliga och teknikerna som används för att få dig att klicka har blivit än mer sofistikerade.

Interaktiv fråga

Vad kan vara ett bra tips för att undvika att drabbas av skadlig kod (virus så som till exempel trojaner och maskar)?

- o Se till att bara använda de program som finns installerade på datorn.
- ✓ Klicka inte på okända länkar eller på okända bilagor i din e-post.
- o Surfa enbart på adresser som slutar på .se eller .nu.

Hur gör din organisation?

Ta reda på vad som gäller i din organisation.

Vem rapporterar du till om du har använt ett okänt USB-minne, klickat på en olämplig länk eller öppnat en okänd bilaga?

Hur gör din organisation? Fyll i checklistan!

09 Utanför arbetsplatsen

Ingress

Det är viktigt att du tänker säkert även utanför arbetsplatsen, till exempel när du arbetar från ett café eller reser i jobbet. Vet du hur du ska göra för att arbeta lika säkert utanför arbetsplatsen som inne på kontoret?

Film: Utanför arbetsplatsen

Det är vanligt att man jobbar på distans eller reser i jobbet. Även utanför arbetsplatsen är det viktigt att du tänker säkert. Låna inte ut din dator, surfplatta, USB-minne eller mobiltelefon som du använder i arbetet till andra. Undvik att utsätta din information för skadlig kod eller olovlig dataöverföring, till exempel genom att använda en kabel som bara leder ström och inte data när du laddar din mobil utanför arbetsplatsen. När du surfar utanför din arbetsplats tänk på att i första hand använda en VPN-tjänst, ett virtuellt privat nätverk, om organisationen har ett sånt, och i andra hand använda din mobildata. Eftersom publika wifi-nätverk går att avlyssna bör du undvika dem. Trevlig resa!

Interaktiv fråga

Vad är ett VPN?

- ✓ En teknik som används för att skapa en säker förbindelse mellan två punkter i ett osäkert nätverk.
- o En digital tunnel som används för att lagra information.
- o En virtuell personlig nod som visar vad du befinner dig när du inloggad.

Hur gör din organisation?

Ta reda på vad som gäller i din organisation.

Vilka regler gäller för hur du arbetar informationssäkert utanför arbetsplatsen?

Hur gör din organisation? Fyll i checklistan!

10 När det blir fel

Ingress

Ibland blir det fel. Känner du att det är okej att rapportera incidenter till din organisation? Vet du hur och till vem du ska rapportera?

Film: När det blir fel

Ibland blir det fel. De flesta incidenter beror på felaktig hantering av information eller rena olyckor. Det är viktigt att ledningen ser avvikelser och incidenter som ett tillfälle för organisationen att dra lärdom och förbättra sina arbetssätt. I organisationer med en sund informationssäkerhetskultur ska det kännas bra att rapportera problem och händelser. Även när det nästan gått fel. Efter att du och dina kolleger rapporterat ska ni få återkoppling. Det är bättre att rapportera en gång för mycket än en gång för lite.

Interaktiv fråga

Du har råkat klicka på en länk som släcker din dator. Vad gör du?

- o Drar ut sladden och försöker sen slå på datorn igen.
- o Säger till din kollega.
- ✓ Du rapporterar vad som hänt genom rätta kanaler.

Hur gör din organisation?

Ta reda på vad som gäller i din organisation.

Vem rapporterar du incidenter till och hur ska du rapportera?

Hur gör din organisation? Fyll i checklistan!

Avslut

Du har nu tagit dig igenom hela Disa. Bra jobbat! Checklistan kan du använda som ett underlag för att komma ihåg vad som gäller i just din organisation. Kanske kan du diskutera den tillsammans med kollegor eller med din chef för att förbättra ert eget informationssäkerhetsarbete?

Vill du veta mer om vad ett systematiskt informationssäkerhetsarbete är? Ladda ner MSB:s publikation ”Metodstödet – en översikt” eller gå till vår hemsida: www.informationssäkerhet.se”.

Lycka till!

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984