Lunds kommun

Rapport: Informationssäkerhet i praktiken
December 2021

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Lunds kommun har EY genomfört en granskning för att testa hur väl kommunens arbete med IT- och informationssäkerhet har kommunicerats till medarbetare i praktiken, exempelvis genom utbildningar och instruktioner. Granskningens syfte har varit att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet. Detta genom att bedöma i vilken utsträckning en angripare riskerar att komma åt kommunens IT-miljöer genom angrepp via e-post. De följande revisionsfrågorna har legat till grund för granskningen:

- Hur väl hanterar kommunstyrelsen hotet från attacker genom falska email, så kallad phishing?
- Kan kommunstyrelsens säkerhetsarbete kopplat till attacker med falska email anses vara ändamålsenligt?

Granskningen genomfördes från september 2021 till december 2021 och baserades på en simulerad cyberattack via e-post, där det finns en risk att medarbetare inom kommunen luras att lämna ut användarinformation till en falsk avsändare, i en så kallad phishingattack. Granskningen utformades och utfördes av EY tillsammans med representanter från kommunen. Metoden bygger på EY:s etablerade ramverk över hur en organisation arbetar med informationssäkerhet och EY:s beprövade metodik för att genomföra en simulerad phishingattack. Resultaten analyserade tre huvudområden: 1) Mottagare som klickat på länken i e-postmeddelandet, 2) Mottagare som uppgav användarinformation på landningssidan, samt 3) Mottagares medvetenhet kring informationssäkerhet och phishing. Dessa områden jämfördes sedan mot på förhand definierade acceptansnivåer och med vad EY anser är en godtagbar standard i offentlig sektor.

Baserat på genomförd granskning bedömer EY att det finns betydande brister i utbildning och medvetenhet inom informationssäkerhet i Lunds kommun. Granskningsresultatet visar att kommunen ligger på en nivå markant under det man bör förvänta sig av en kommun av denna storlek och karaktär. Slutsatsen bygger på den typ av verksamhet som bedrivs samt på känslighetsgraden av den information, exempelvis personuppgifter, som kommunen behandlar i dess dagliga verksamhet. I relation till de på förhand bestämda acceptansnivåerna som bestämts i samråd mellan EY och kommunen löper Lunds kommun en mycket hög risk att utsättas för en fullbordad phishingattack. Kommunen rekommenderas att vidta åtgärder för att stärka utbildning och medvetenhet hos sina medarbetare, samt åtgärda svagheter i motståndskraften mot phishingattacker. Detta för att undvika förluster av känslig information, negativt rykte eller andra betydande konsekvenser. Utifrån resultatet av granskningen har EY valt att presentera tre övergripande rekommendationer som Lunds kommun bör fokusera sitt arbete på framöver:

- Ett strukturerat och regelbundet arbete med utbildningar i informationssäkerhet.
- Teoretiska samt praktiska övningar inom området phishing.
- Tydliggörande av rapporteringsvägar, samt kommunikation av betydelsen att rapportera säkerhetsincidenter för alla medarbetare.

Innehållsförteckning

1. Bakgrund

Lunds kommun och dess olika nämnder och förvaltningar hanterar stora mängder digital information. Detta ger många nya möjligheter i form av effektivare förvaltning, uppföljning och utökad service till medborgare, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig, har tillräckligt starkt skydd samt är spårbar.

I tidigare granskningar har kommunens revisorer identifierat risker relaterat till kommunens övergripande arbete med IT- och informationssäkerhet samt sårbarheter kopplat till verksamhetskritiska system inom kommunen. En av de mer kritiska observationerna var att utbildningen av kommunens medarbetare inom IT- och informationssäkerhet behöver förbättras. Revisorerna har därför valt att genomföra en granskning för att testa hur väl kommunens arbete med IT- och informationssäkerhet har kommunicerats till medarbetarna i praktiken.

En sådan granskning genomförs genom att EY simulerar en attack där falska email skickas ut till medarbetarna, en så kallad "phishingattack". Genom ett fullgott informationssäkerhetsarbete bör medarbetarna kunna identifiera ett sådant angrepp och veta hur de ska agera för att hantera och rapportera med bibehållen säkerhet. Genom att analysera hur många som agerade korrekt kan revisorerna få en bild av hur väl utbildning och medvetenhet fungerar i praktiken.

1.1 Phishing

Digitalisering leder till en ökad risk relaterad till informationssäkerhet. Cyberkriminella aktörer väljer i en hög utsträckning att inte enbart attackera teknologin i en organisation, utan även människorna i den. Cyberkriminella utför social manipulation genom att utnyttja mänskliga svagheter som rädsla och förtroende för att utvinna känslig information som är viktig att skydda. Cyberkriminella kan även med social manipulation sprida skadlig kod som kan tillfoga en organisation, dess intressenter, och samhället stor förstörelse. Under den osäkra situationen av COVID-19 har EY sett en ökning av denna typ av cyberkriminalitet, särskilt genom phishing. Detta innebär att den mänskliga aspekten blir avgörande för att säkerställa ett adekvat skydd av en organisations tillgångar, samt för att uppfylla gällande lagkrav om informationssäkerhet och integritet.

En fullbordad attack av phishing kan innebära stora konsekvenser för en organisation, både finansiellt och socialt, som ett försämrat anseende och rykte. Det är därmed viktigt att vara proaktiv och bekämpa det ökade hotet av phishing. Risken för en fullbordad attack av phishing minskas om medarbetare inom en organisation är medvetna om hotet av phishing, har kunskapen att kunna identifiera indikationer av ett falskt e-postmeddelande med fientligt uppsåt, samt har en tydlig rapporteringsväg att följa för att rapportera eventuellt misstänkta e-postmeddelanden. Att kontinuerligt genomföra medvetenhetsträning inom informationssäkerhet för att medarbetare ska upptäcka och reagera på hotet från phishing är ett alternativ för att mitigera riskerna från denna typ av cyberattacker.

1.2 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet genom att testa utbildning och medvetenhet hos medarbetarna inom kommunen. Vidare är syftet också att bedöma i vilken utsträckning en angripare riskerar att komma åt kommunens IT-miljöer genom angrepp via e-post. De följande revisionsfrågorna har legat till grund för granskningen:

- Hur väl hanterar kommunstyrelsen hotet från attacker genom falska email, så kallad phishing?
  - Finns det riktlinjer för denna typ av IT-säkerhetshot?
  - Är riktlinjerna i så fall kända i organisationen?
  - Genomförs det fortlöpande utbildningar bland medarbetarna för att höja medvetenheten av IT-säkerhetshot?
- Kan kommunstyrelsens säkerhetsarbete kopplat till attacker med falska email anses vara ändamålsenligt?

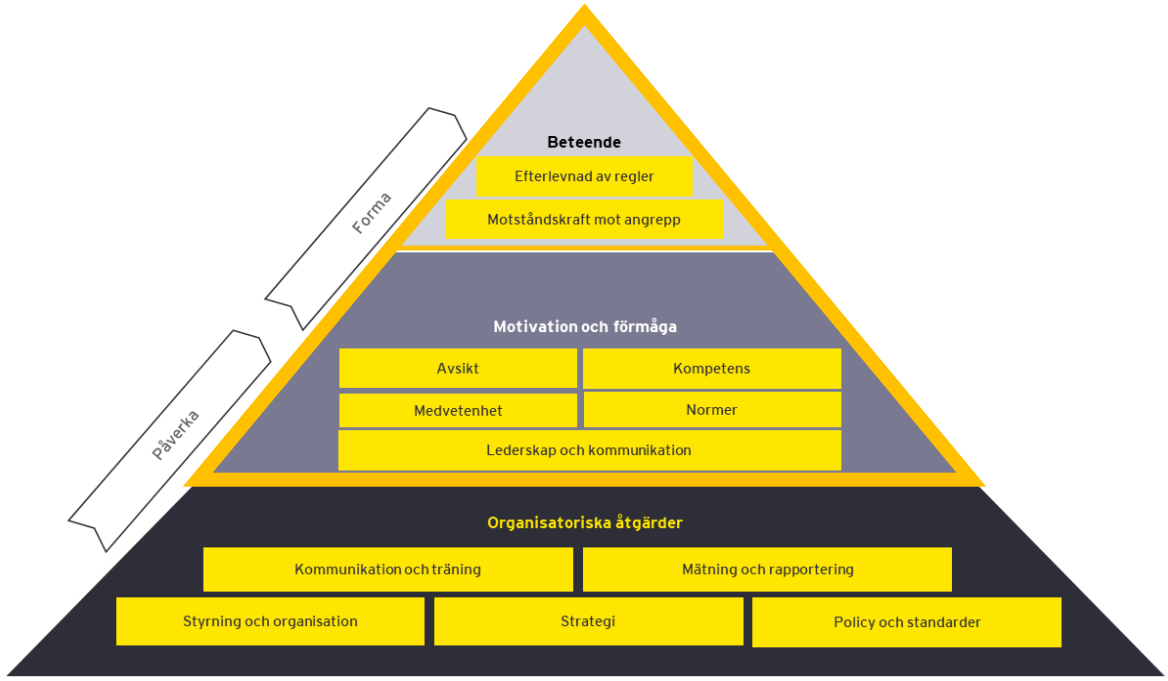
1.3 Avgränsningar

Granskningen är avgränsad till att ge en bild över hur sårbar kommunen är för attacker riktade mot kommunens medarbetare via e-post. Det ges alltså inte någon helhetsbild av kommunens totala arbete inom IT- och informationssäkerhet utan syftet är att ge en mer detaljerad bild av ett begränsat område. Ingen teknisk testning har heller utförts för att granska effektiviteten i kommunens skalskydd, dvs. hur väl existerade och inbyggda säkerhetskontroller fungerar för att identifiera och stoppa falska e-postmeddelanden.

1.4 Metod och genomförande

Granskningen bygger på EY:s etablerade ramverk för hur en organisation arbetar med informationssäkerhet. *Figur 1* nedan visar hur organisatoriska åtgärder som exempelvis kommunikation och utbildning, styrning, samt riktlinjer ligger till grund för nivån av informationssäkerheten i en organisation. De organisatoriska åtgärderna påverkar sedan i sin tur motivationen och förmågan hos anställda i en organisation att agera i enlighet med de riktlinjer organisationen önskar. Motivationen och förmågan hos anställda baseras på flera olika faktorer som ledarskap och kommunikation, avsikt, samt medvetenhet och kompetens kring informationssäkerhet. Motivationen och förmågan hos de anställda i Lunds kommun har i denna granskning utvärderats genom en enkät som distribuerades efter genomförd övning. Enkätens syfte var att mottagarna själva skulle reflektera över deras medvetenhet, kunskap och beteende kring informationssäkerhet.

Motivationen och förmågan hos anställda i en organisation formar i sin tur deras beteende relaterat till informationssäkerhet, närmare bestämt hur väl man efterlever regler och hur stark motståndskraften är mot ett potentiellt angrepp inom organisationen. Beteendet hos anställda i Lunds kommun har i denna granskning utvärderats genom att utföra en simulerad phishingattack. Notera att granskningen i sin helhet huvudsakligen fokuserar på de två översta delarna av ramverket: beteende samt motivation och förmåga.



Figur 1: EY:s ramverk för bedömning av en organisations informationssäkerhet

Nedan följer en mer detaljerad beskrivning av EY:s metodik för att utföra en phishingövning och en detaljerad beskrivning av hur övningen genomfördes.

1.4.1 Metod

EY använder en beprövad metodik för att genomföra och analysera en simulerad phishingattack. Övningen sätts upp med hjälp av ett verktyg som används för att skicka ut ett e-postmeddelande till den definierade målgruppen och för att samla in data kring det faktiska utfallet. Insamlad information jämförs sedan mot på förhand definierade acceptansnivåer, samt vad EY anser är en godtagbar standard i offentlig sektor. Den information som ligger till grund för granskningen har samlats in av EY i möten med utvalda nyckelpersoner som arbetar med informationssäkerhet inom Lunds kommun.

För att besvara revisionsfrågorna har EY granskat tre huvudområden enligt nedan:

- **Mottagare som klickade på länken i e-postmeddelandet** – EY har granskat hur många mottagare av det förfalskade e-postmeddelandet som klickade på den inbäddade länken till landningssidan (internetsida). Detta för att få en förståelse för kommunens motståndskraft mot hotet av phishing, samt hur god kunskapsnivån hos kommunens medarbetare är för att kunna identifiera ett e-postmeddelande från en falsk avsändare. EY bedömer att detta är ett viktigt område att granska då riskerna för att cyberkriminella kan utvinna känslig information, implementera skadlig kod, eller attackera en organisations IT-infrastruktur ökar avsevärt om en mottagare klickar på en skadlig länk eller laddar ner en bilaga i ett e-postmeddelande skickat från en okänd avsändare.
- **Mottagare som uppgav användarinformation på landningssidan** – EY har granskat hur många mottagare av det förfalskade e-postmeddelandet som initialt klickade på länken inbäddad i e-postmeddelandet, för att sedan uppge användarinformation på

den förfalskade landningssidan. Detta för att skapa en förståelse för hur stark kommunens motståndskraft är mot angrepp av phishing, samt för att mäta kunskapsnivån hos kommunens medarbetare att kunna identifiera en förfalskad landningssida från en okänd domän. EY bedömer att detta är ett viktigt område att granska då riskerna för att cyberkriminella kan utvinna känslig information och ta sig in i en organisations IT-infrastruktur ökar avsevärt om en medarbetare delar med sig av sin användarinformation som kan leda till en organisations tillgångar.

- **Mottagares medvetenhet kring informationssäkerhet och phishing** - EY har med hjälp av kommunen distribuerat en enkät med syftet att skapa sig en uppfattning om motivationen och kunskapen relaterat till denna typ av cyberhot hos mottagarna av e-postmeddelandet. Enkäten omfattar frågor kring e-postmeddelandet som användes i simuleringen och säkerhetskulturen på kommunen i form av utbildning och medvetenhet, styrande dokument och rapportering av säkerhetsincidenter. EY bedömer detta som ett viktigt område att granska, då det visar på hur medvetna medarbetarna inom kommunen är om hotet av phishing, samt dess kunskaper att agera i enlighet med kommunens riktlinjer när ett falskt e-postmeddelande upptäcks. Det visar sig att en tidig rapportering av ett misstänksamt e-postmeddelande tillåter en organisation att omedelbart upptäcka en cyberattack av detta slag, utreda dess omfattning, och sätta in adekvata skyddsåtgärder för att lindra attackens potentiella konsekvenser.

1.4.2 Genomförande

Övningen har utformats och genomförts av specialister inom IT- och informationssäkerhet från EY, tillsammans med utvalda representanter från Lunds kommun. De utvalda representanterna från kommunen har givits möjlighet att faktagranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekta fakta. Nedan följer en ingående beskrivning av respektive huvudmoment för att förbereda, utföra och analysera den simulerade attacken.

1.4.2.1 E-postmeddelande och landningssida

En simulerad phishingattack bygger på att ett e-postmeddelande skickas ut till en utvald målgrupp. E-postmeddelandet kan vara utformat på olika sätt baserat på övningens syfte. E-postmeddelandet kan exempelvis innehålla en länk som leder vidare till en landningssida eller inkludera en länk som initierar en nerladdning av en fil. E-postmeddelanden som inkluderar en länk till en landningssida testar vanligtvis hur villiga anställda är att dela med sig av användarinformation som inloggningsuppgifter eller att ladda ner okända filer.

För att bestämma hur e-postmeddelandet skulle utformas hölls inledningsvis möten tillsammans med kommunens representanter. Beslutet föll på att inkludera en länk i e-postmeddelande som hänvisade till en landningssida. På landningssidan uppmanades mottagaren att uppge inloggningsuppgifter (e-postadress samt lösenord) till sin inkorg. Om en mottagare valde att fylla i sina användaruppgifter på landningssidan, dirigerades de vidare till ytterligare en landningssida som informerade mottagaren att de deltagit i en simulerad phishingattack. Syftet med den informerande landningssidan är att skapa medvetenhet kring informationssäkerhet i organisationen och informera de anställda inom hotet av phishing. För e-postmeddelandet som skickades ut och de båda landningssidorna, se *bilaga 1* och *bilaga 2*.

1.4.2.2 Målgrupp och utskick

Målgruppen för en simulerad phishingattack kan variera beroende på övningens syfte. E-postmeddelandet kan exempelvis vara riktat mot utvalda avdelningar eller bolag baserat på deras risknivå. E-postmeddelandet kan också skickas ut till samtliga anställda för att på så sätt skaffa sig en övergripande bild av kommunens motståndskraft och de anställdas medvetenhet.

I samråd med kommunens representanter beslutades det att skicka ut e-postmeddelandet till ett urval av kommunens samtliga medarbetare, då det stora antalet anställda inom kommunen hade inneburit höga interna belastningar på rapporteringsvägar samt informationssäkerhetsansvariga. För att få en övergripande bild av nivån på informationssäkerhet i praktiken över alla kommunens förvaltningar beslutades det därmed att genomföra ett urval av mottagare, vilket motsvarade 20 procent av det totala antalet anställda från samtliga förvaltningar. Detta resulterade i att 2331 medarbetare inom kommunen deltog i övningen och att samtliga förvaltningar representerades i granskningen. EY noterade att 4 användare inkluderats i listan av mottagare från ett helägt bolag inom kommunen. Då endast anställda från kommunens förvaltningar inkluderas i urvalet baserades analysen på totalt 2327 mottagare.

Innan det faktiska e-postmeddelandet skickades ut hölls ett testmöte där den simulerade attacken testades för att säkerställa att e-postmeddelandet gick igenom skalskyddet och skulle nå fram till mottagarna. Den tekniska genomgången inkluderade behov av vitlistning, spamfilter och potentiell rate limiting. EY genomförde sedan simuleringen den 2021-10-19, då e-postmeddelandet skickades till samtliga utvalda mottagare. Simuleringen var aktiv i en veckas tid, fram till att den stängdes den 2021-11-05.

1.4.2.3 Rapportering

Att skydda sig mot hotet från en phishingattack kan vara svårt och kräver samverkan av olika faktorer. En viktig komponent är att effektiva rapporteringsvägar existerar och att anställda är medvetna om dessa. Åtgärder bör vidtas skyndsamt då hotet är som störst under den initiala tiden efter att e-postmeddelandet mottagits. Det är också av stor vikt att personer som förmodar att de blivit utsatta för angrepp vidtar nödvändiga åtgärder för att ändra inloggningsuppgifter som en angripare kan ha fått tillgång till.

Inom Lunds kommun ska rapporteringen av ett förmodat falskt e-postmeddelande rapporteras till kommunens interna servicedesk eller relevant personal som arbetar med informationssäkerhet. Rapporteringen kan ske via valfritt kommunikationsmedel. Notera att detta i dagsläget är en inofficiell rapporteringsväg, då dessa rutiner för hur en anställd ska rapportera ett e-postmeddelandet och hantera en potentiell phishingattack inte är dokumenterade. Kommunen har delgivit EY en dokumenterad rutin för att rapportera ett misstänksamt e-postmeddelande via Microsoft rapporteringstjänst. Enligt representanter från kommunen är dock detta inte en förankrad rutin som användas i det dagliga arbetet inom organisationen.

1.4.2.4 Enkät

Efter avslutad simulering distribuerade EY ett urval av enkätfrågor via kommunens interna enkätverktyg till mottagarna av e-postmeddelandet. Detta för att skapa en förståelse för motivationen och förmågan hos kommunens anställda för att identifiera ett falskt e-postmeddelande, samt agera i enlighet med befintliga riktlinjer för att limitera en pågående phishingattack. Syftet med enkäten var att mottagarna skulle reflektera över sina tankar, åsikter och attityder kring deras vanor, kunskap och medvetenhet av hotet från phishing samt karaktären av en phishingattack. Även säkerhetskulturen inom kommunen utvärderades till viss del genom enkäten, då den inkluderade områden som ledarskap, riktlinjer och utbildning kring informationssäkerhet.

Enkäten inkluderade även uppföljande frågor om den genomförda övningen, för att EY skulle kunna skapa sig en förståelse för hur mottagarna antingen identifierade det falska e-postmeddelandet eller inte, och om de i sin tur klickade på den falska länken. Detta med syftet att förstå hur stor kunskap de anställda inom kommunen har för att kunna identifiera ett e-postmeddelande skickat från en falsk avsändare. Se *bilaga 4* för enkäten som användes i samband med övningen.

1.4.2.5 Risknivåer och acceptansnivåer

För att tolka resultaten av en simulerad phishingattack krävs en förståelse för potentiella risker av en fullbordad attack (risknivåer) och mottagarens relativa benägenhet att acceptera riskerna (acceptansnivåer). Risken för en fullbordad attack kan exempelvis vara mer omfattande för en större kommun då dessa besitter mer känslig information och större finansiell kraft. Det kan också vara skillnader inom en kommun, där vissa förvaltningar kan ha mindre risk än andra baserat på typen av verksamhet som bedrivs. Se *tabell 1* för definitioner av risknivåer som EY har använt under genomförd granskning:

Tabell 1: Risknivåer för phishingövning

Mycket hög risk	En mycket hög risk för, och i samband med, en phishingattack existerar. Kommunen rekommenderas att omgående vidta åtgärder för att åtgärda svagheter i motståndskraften mot phishingattacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Hög risk	En hög risk för, och i samband med, en phishingattack existerar. Kommunen rekommenderas att vidta åtgärder för att utvärdera och åtgärda svagheter i motståndskraften mot phishingattacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Medel risk	En medel risk för, och i samband med, en phishingattack existerar. Kommunen rekommenderas att utvärdera och förbättra motståndskraften mot phishingattacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Låg risk	En låg risk för, och i samband med, en phishingattack existerar. Kommunen rekommenderas att arbeta vidare med att kontinuerligt säkerställa en hög motståndskraft mot phishingattacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.

Innan en simulerad phishingattack påbörjas är det viktigt att översätta de olika risknivåerna till specifika mätetal anpassade för den aktuella organisationen, vilket kallas för acceptansnivåer. Notera att acceptansnivåerna för andelen mottagare som anger användarinformation på landningssidan generellt sett är lägre än för andelen mottagare som klickar på länken i e-postmeddelandet. Detta då EY anser att risken för att en fullbordad phishingattack är högre om en cyberkriminell får tillgång till användardata och därmed potentiellt kommunens IT-miljöer. För den simulerade övningen definierades acceptansnivåer i samråd mellan EY och kommunens representanter genom att omvandla risknivåerna till specifika procentandelar, se *bilaga 3*.

1.4.3 Tidsplan

Granskningen genomfördes från september 2021 till december 2021, se *tabell 2* nedan för granskningens tidsplan.

Tabell 2: Tidsplan

Förberedelser och planering	September 2021
Test och utskick	Oktober - november 2021
Rapportskrivning samt intern kvalitetssäkring	November 2021
Justering samt färdigställande av rapport	November 2021
Avrapportering och slutpresentation	December 2021

2. Analys

En phishingattack kan genomföras på många olika sätt vilket kan påverka resultatet och eventuella konsekvenser av attacken. Beroende på vad en cyberkriminell aktör har för målsättning med en attack kan den vara mer eller mindre riktad till specifika personer eller avdelningar inom kommunen. Phishingattackens utformning påverkar därmed resultatet och bör vägas in i analysen. I följande kapitel analyseras resultatet av den simulerade attack som EY gemensamt med kommunen utformat. Analysen presenteras i tre delar baserat på tre huvudområden: 2.1 Mottagare som klickat på länken i e-postmeddelandet, 2.2 Mottagare som uppgav användarinformation på landningssidan, samt 2.3 Mottagares medvetenhet kring informationssäkerhet och phishing.

2.1 Mottagare som klickade på länken i e-postmeddelandet

I detta avsnitt presenteras andelen mottagare som klickade på länken i e-postmeddelandet. Resultatet av den simulerade attacken visar att 33 procent av samtliga mottagare klickade på den inbäddade länken i e-postmeddelandet. Resultatet av granskningen visar att Lunds kommun löper en mycket hög risk att utsättas för phishingattacker i relation till de på förhand definierade acceptansnivåerna.

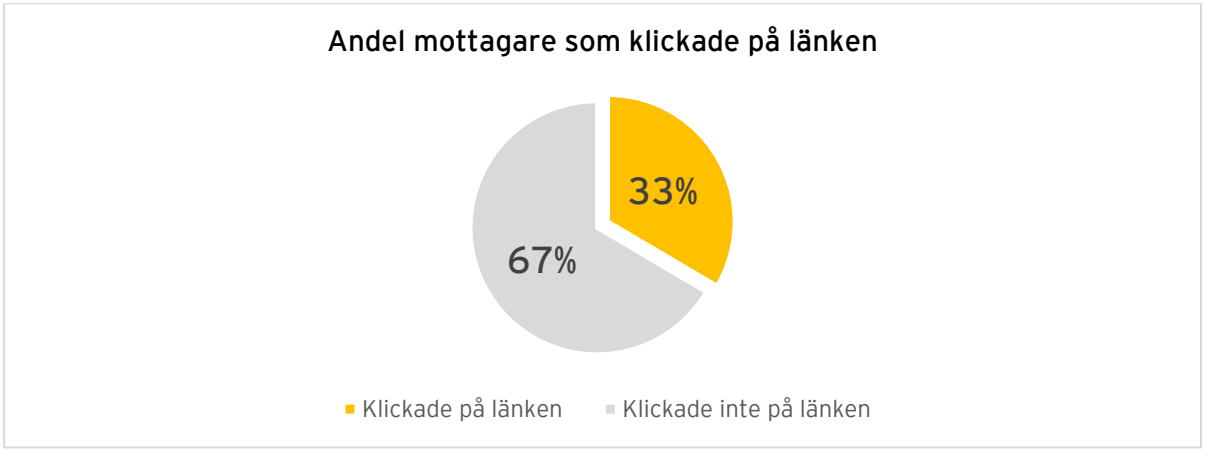
Lunds kommun hade i samråd med EY på förhand bestämt acceptansnivåer baserat på verksamhetens omfattning och dess befintliga arbete kring medvetenhet av informationssäkerhet. *Tabell 3* nedan beskriver de beslutade acceptansnivåerna för andelen mottagare som klickar på länken.

Tabell 3: Acceptansnivåer för andelen mottagare som klickar på länken

Riskanalys	Acceptansnivå (%)
Mycket hög risk	>15%
Hög risk	10-15%
Medel risk	5-10%
Låg risk	<5%

2.1.1 Resultat av simulering

E-postmeddelandet skickades till ett urval av medarbetare inom kommunens samtliga 12 förvaltningar. Av 2327 mottagare klickade 778 på länken i e-postmeddelandet, vilket motsvarar 33 procent av samtliga mottagare, se *figur 2* nedan. Det här resultatet innebär enligt acceptansnivåerna att Lunds kommun och dess förvaltningar löper en mycket hög risk att utsättas för en fullbordad attack av phishing.



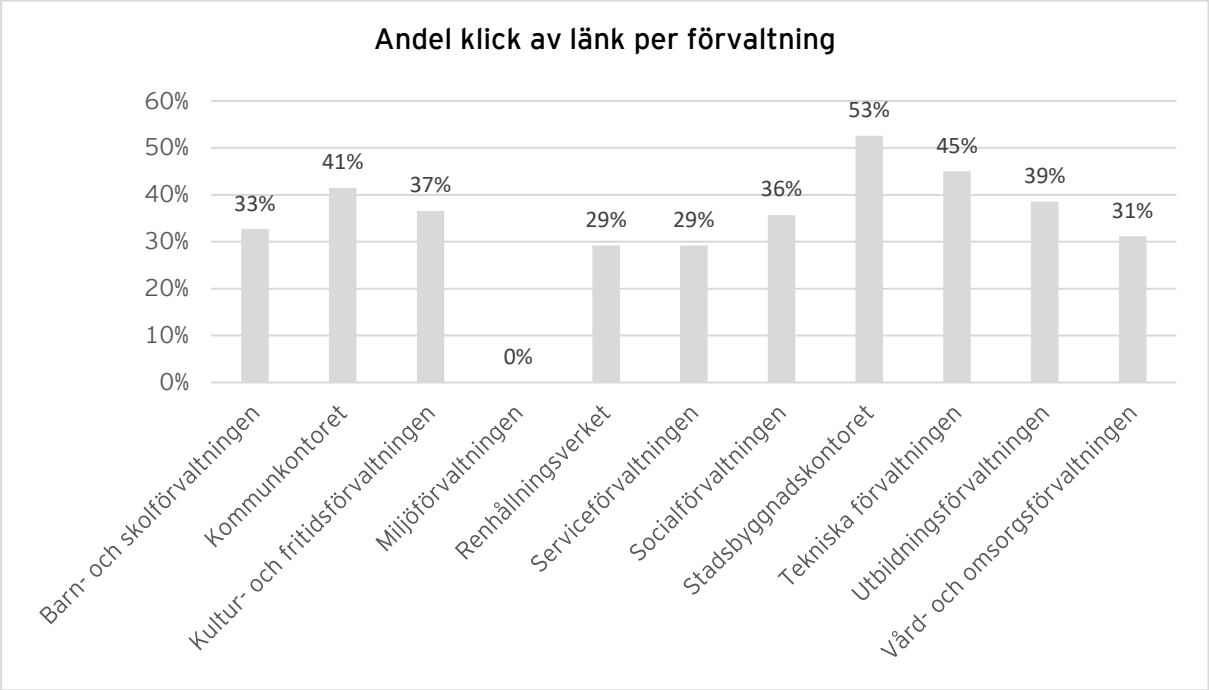
Figur 2: Fördelningen av andel mottagare som klickade på länken i e-postmeddelandet (%).

Simuleringen var aktiv under en veckas period. I *figur 3* illustreras andelen klick av länken per dag, där det visualiseras att 73 procent av alla mottagare klickade på länken i e-postmeddelandet under simuleringens första dag. EY noterade att då simuleringen inleddes under en fredag, sjöng antalet klick på länken markant under de nästkommande två helgdagarna. EY noterade sedan en liten ökning igen, under följande måndag, då 12 procent av mottagarna klickade på länken i e-postmeddelandet. Den här trenden är enligt EY förväntad i en simulerad attack då den påkallar omedelbara handlingar av mottagaren.

Figur 3: Andelen klick av länk i e-postmeddelandet under simuleringens aktiva period (%).

Figur 4 visar andelen klick av länken i e-postmeddelandet per förvaltning. EY noterar att andelen klick per förvaltning generellt är på en hög nivå i jämförelse med de på förhand bestämda acceptansnivåerna. Det här innebär att de flesta av förvaltningarna har medarbetare som klickade på länken i e-postmeddelandet. EY noterade att stadsbyggnadskontoret var förvaltningen med den högsta andelen mottagare som klickat på länken. 10 av 19 mottagare klickade på länken, vilket motsvarar 53 procent av deras totala mottagarantal. I relation till de förutbestämda acceptansnivåerna löper samtliga förvaltningar en mycket hög risk att utsättas för en fullbordad phishingattack, med undantag för miljöförvaltningen som löper en låg risk för detta då inga mottagare klickade

på länken i e-postmeddelandet. Notera dock att e-postmeddelandet skickades till ett relativt lågt antal mottagare (7) hos Miljöförvaltningen.



Figur 4: Fördelning av mottagare som klickade på länken per förvaltning (%). Notera att andel mottagare som klickat på e-postmeddelandet baseras på antalet e-postmeddelanden som skickades till respektive förvaltning.

2.2 Mottagare som uppgav användarinformation på landningssida

I det här avsnittet presenteras andelen mottagare som efter att de klickat på länken i e-postmeddelandet även uppgav användarinformation i form av e-postadress samt lösenord på landningssidan. Resultatet av den simulerade attacken visar att 19 procent av mottagarna uppgav sin användarinformation på den förfalskade landningssidan. I relation till de på förhand definierade acceptansnivåerna (se *tabell 4*) indikerar resultatet på att Lunds kommun löper en mycket hög risk att utsättas för en fullbordad phishingattack.

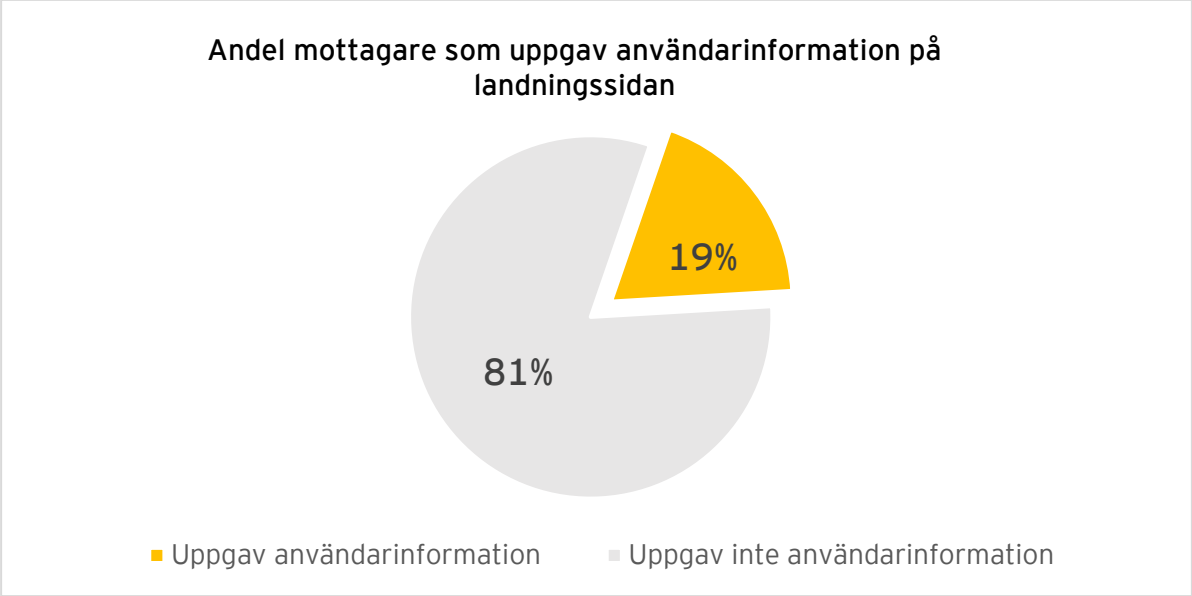
Lunds kommun hade i samråd med EY på förhand bestämt acceptansnivåer baserat på verksamhetens omfattning och dess befintliga arbete kring medvetenhet av informationssäkerhet. *Tabell 4* beskriver de beslutade acceptansnivåerna för andelen mottagare som uppger användarinformation.

Tabell 4: Acceptansnivåer för mottagare som uppger användarinformation på landningssidan

Riskanalys	Acceptansnivå (%)
Mycket hög risk	>6%
Hög risk	4-6%
Medel risk	2-4%
Låg risk	<2%

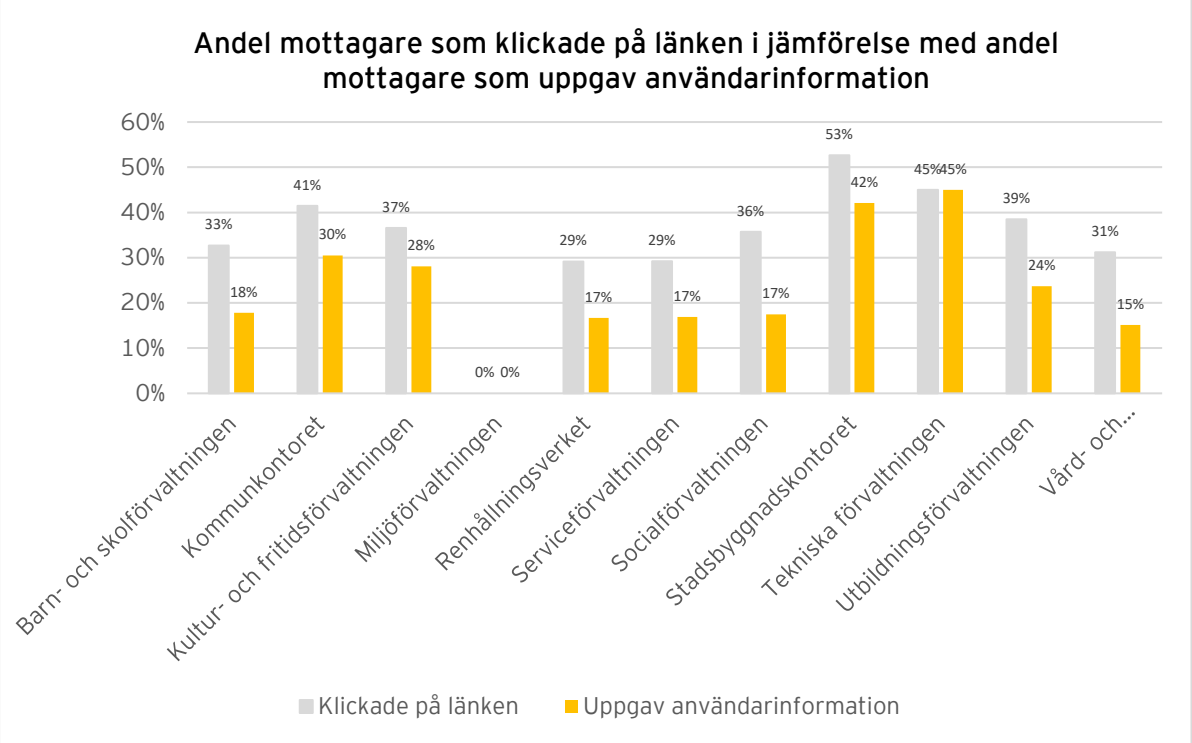
2.2.1 Resultat av simulering

Av 2327 mottagare var det 436 medarbetare som klickade på länken och sedan uppgav sin användarinformation i form av användarnamn och lösenord på landningssidan. Det motsvarar 19 procent av alla mottagare, se *figur 5*. I jämförelse med acceptansnivåerna i *tabell 4*, löper därmed Lunds kommun en mycket hög risk att utsättas för en fullbordad phishingattack.



Figur 5: Fördelningen av andel mottagare som uppgav användarinformation på landningssidan (%).

Figur 6 visar en jämförelse över andelen mottagare som klickade på länken i e-postmeddelandet i relation till andelen mottagare som uppgav användarinformation på landningssidan för respektive förvaltning. Som tidigare noterat var stadsbyggnadskontoret den förvaltning där flest mottagare procentuellt klickade på länken, där även 42 procent av förvaltningens mottagare lämnade användarinformation på landningssidan. Tekniska förvaltningen hade den högsta andelen mottagare som uppgav användarinformation på landningssidan då de utgjorde 45 procent av förvaltningens totala mottagarantal. EY noterade även att samtliga (9 av totalt 20 mottagare) på Tekniska förvaltningen som hade öppnat e-postmeddelandet och klickat på länken även hade lämnat användardata. Baserat på de bestämda acceptansnivåerna löper samtliga förvaltningar, med undantag för Miljöförvaltningen, en mycket hög risk att utsättas för en fullbordad phishingattack. Enligt acceptansnivåerna löper Miljöförvaltningen en låg risk för att utsättas för en attack, både när det kommer till andelen som klickat på länken och andelen som lämnat sin användarinformation.



Figur 6: Jämförelse av mottagare som klickade på länken i relation till mottagare som lämnade användarinformation per förvaltning (%). Notera att andelen mottagare baseras på antalet e-postmeddelande som skickades till respektive förvaltning.

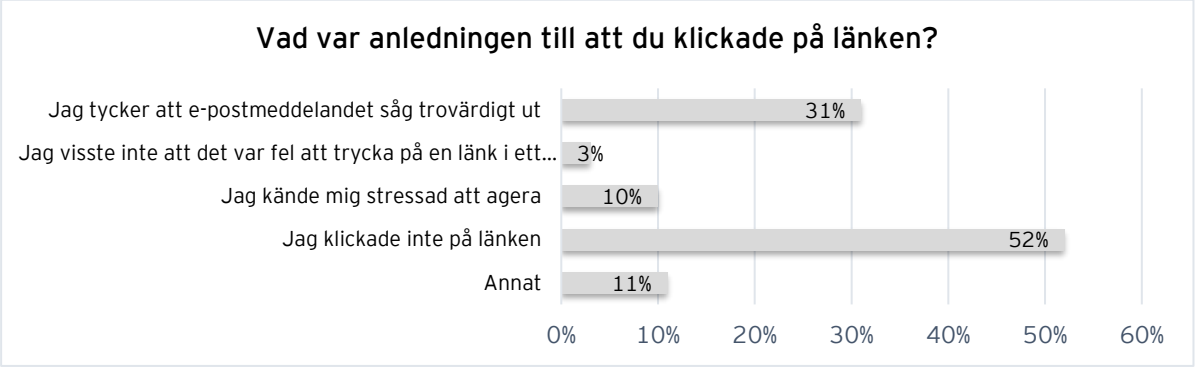
2.3 Mottagares medvetenhet kring informationssäkerhet och phishing

I detta avsnitt presenteras resultatet av enkäten som distribuerades efter avslutad simulering till alla mottagare av e-postmeddelandet. Syftet med enkäten var att skapa en övergripande förståelse för hur medvetna de anställda i Lunds kommun är om informationssäkerhet och phishing. Enkäten inkluderade frågor inom följande två områden: 1) E-postmeddelandet som användes i övningen och vanliga indikatorer av phishing, 2) Säkerhetskulturen på kommunen i form av utbildning och medvetenhet, styrande dokument samt rapportering av säkerhetsincidenter. Enkäten skickades ut till samtliga deltagare i övningen, varav 439 av dessa mottagare deltog i enkätundersökningen. Notera att i denna analys presenteras ett urval av de enkätfrågor som användes i undersökningen. Se *bilaga 4* för den fullständiga enkäten.

2.3.1 Resultat av enkät

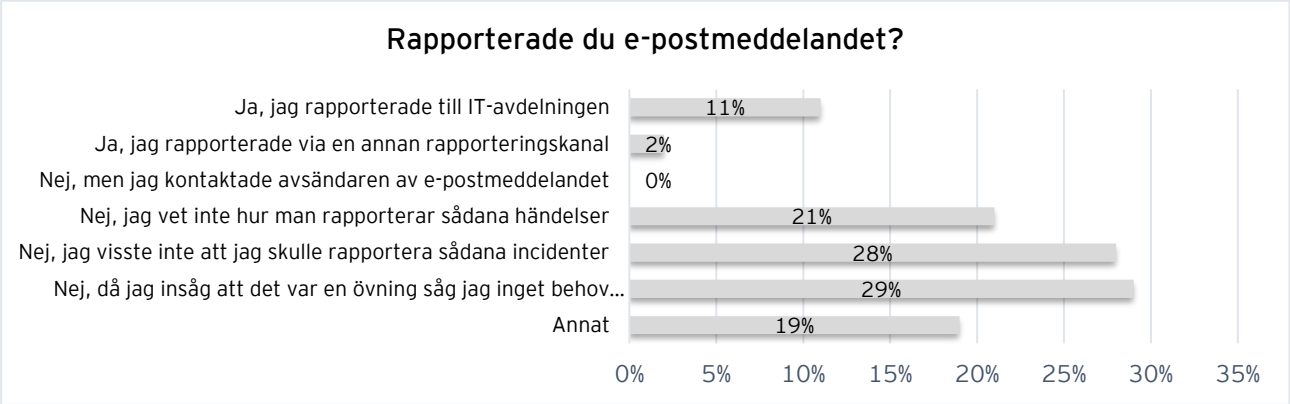
Medarbetares förmåga att identifiera ett falskt e-postmeddelande är av stor vikt för att Lunds kommun ska kunna minimera riskerna för en fullbordad phishingattack. *Figur 7* nedan visar potentiella anledningar till att mottagarna av e-postmeddelandet klickade på den inbäddade länken i e-postmeddelandet. Resultatet visar att 52 procent av de mottagare som deltog i enkäten uppgav att de inte klickat på länken. Vidare visade resultatet att den största anledningen (31 procent) som mottagare uppgav till varför de klickade på länken var för att de ansåg att e-postmeddelandet såg trovärdigt ut. 10 procent av deltagarna uppgav att de klickade på länken för att de upplevde en stress att

agera i enlighet med e-postmeddelandets uppmaning, medan 3 procent av deltagarna uppgav att de inte hade vetskapen om att klicka på en länk kunde innebära negativa konsekvenser.



Figur 7: Resultat av enkätfråga om länken i e-postmeddelandet (%).

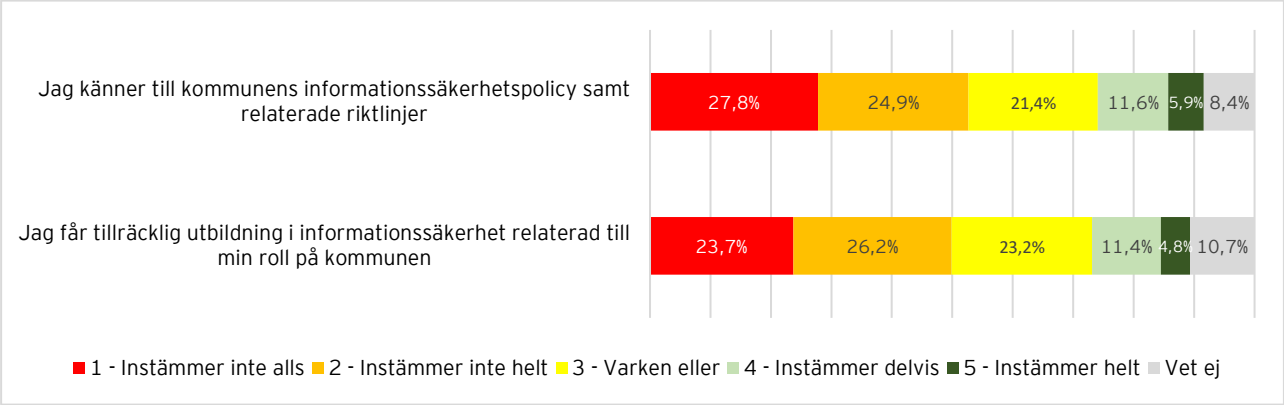
Efter avslutad övning informerade kommunen EY att vissa rapporterade ärenden hade inkommit till olika instanser av kommunen. Då det i dagsläget inte finns en etablerad rapporteringsprocess för phishing hos kommunen loggades inte dessa rapporterade ärenden. Notera att de mottagare som initialt klickade på länken i e-postmeddelandet och sedan uppgav sin användarinformation på landningssidan blev informerade att det var en pågående övning, något som EY anser kan ha påverkat andelen mottagare som valde att rapportera e-postmeddelandet. Detta visualiseras även i *figur 8* nedan, då 29 procent av enkätdeltagarna uppgav att de inte rapporterade e-postmeddelandet då de var medvetna om att det var en övning och ansåg att det inte var nödvändigt att informera kommunen. Vidare visar resultatet att 28 procent av enkätdeltagarna inte hade vetskapen om att denna typ av incident skulle rapporteras. 21 procent av deltagarna menade att de visste hur de skulle gå tillväga för att rapportera liknande incidenter.



Figur 8: Resultat av enkätfråga om rapportering av e-postmeddelandet (%).

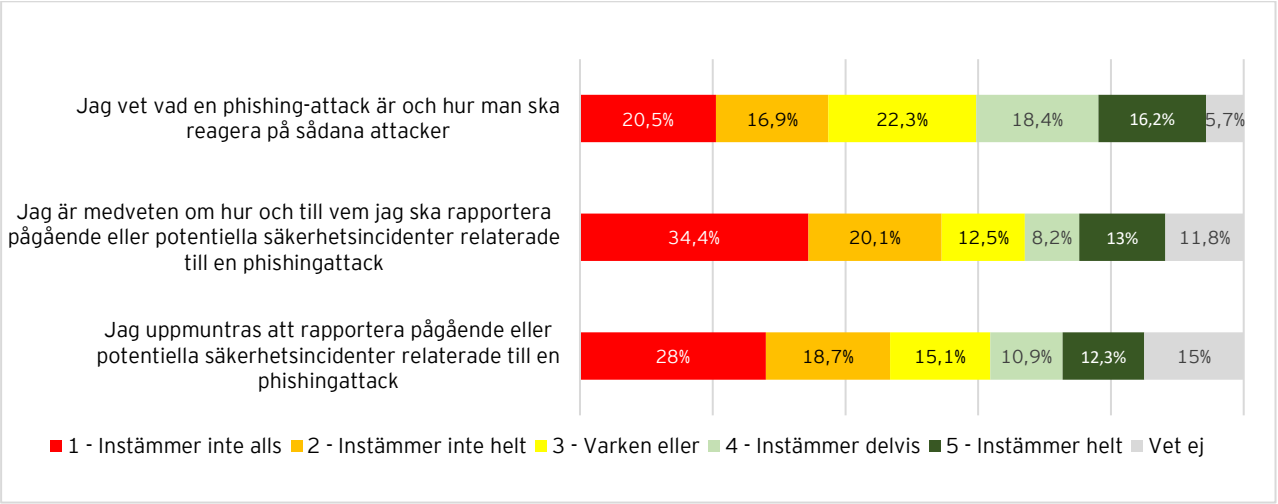
Resultatet av enkäten visade att endast 5,9 procent av deltagarna instämmer helt att de känner till kommunens nuvarande informationssäkerhetspolicy och relaterade riktlinjer, medan majoriteten av deltagarna inte gör det (27,8 procent). Den största andelen av enkätdeltagarna (26,2 procent) uppgav att de inte anser sig få tillräcklig utbildning kring informationssäkerhet relaterat till deras tjänst på kommunen, samtidigt som 4,8 procent

ansåg att de får tillräcklig utbildning kring informationssäkerhet från kommunen. Se *figur 9* för det fullständiga resultatet för dessa påståenden.



Figur 9: Resultat av påståenden om styrande dokument och utbildning inom informationssäkerhet på kommunen (%).

Vidare indikerade resultatet av enkäten att deltagarnas kunskap kring phishingattacker är relativt skiftande. 16,2 procent av deltagarna uppgav att de instämmer helt till påståendet att de vet vad en phishingattack innebär och hur de ska reagera vid en sådan, medan 18,4 procent av deltagarna uppgav att de instämmer delvis till detta. I motsats till detta, svarade 20,5 procent av deltagarna att de inte alls instämmer till detta påstående. EY noterade att majoriteten av enkätdeltagarna (34,4 procent) inte anser sig vara medvetna om hur de ska gå tillväga och vem de ska kontakta för att rapportera en pågående phishingattack. I relation till detta uppgav 28 procent av deltagarna att de inte alls instämde till påståendet att de uppmuntras av kommunen att rapportera potentiella eller pågående säkerhetsincidenter. Samtidigt uppgav 18,7 procent att de inte instämmer helt till påståendet. Se *figur 10* för det fullständiga resultatet för dessa påståenden.



Figur 10: Resultat av påståenden om phishingattacker och rapportering (%).

3. Övergripande rekommendationer

Baserat på genomförd analys bedömer EY att Lunds kommun ligger på en nivå markant under det man bör förvänta sig av en kommun av denna storlek och karaktär. Bedömningen baseras på den typ av verksamhet som bedrivs och på känslighetsgraden av den information, exempelvis personuppgifter, som kommunen behandlar i dess dagliga verksamhet. Kommunen rekommenderas således att vidta åtgärder för att stärka utbildning och medvetenheten hos medarbetarna, samt åtgärda svagheter i motståndskraften mot phishingattacker. Detta för att undvika förluster av känslig information, negativt rykte eller andra betydande konsekvenser. I följande avsnitt presenterar EY tre övergripande rekommendationer som bedöms vara mest relevanta för Lunds kommun. EY rekommenderar att kommunen fokuserar på och påbörjar arbetet med dessa rekommendationer inom 12 månader.

3.1 Strukturerat och regelbundet arbete med utbildningar i informationssäkerhet

Enligt EY:s ramverk för hur en organisation arbetar med informationssäkerhet styrs en organisations motståndskraft av de anställdas motivation och förmågor. Motivation och förmågor formas i sin tur av olika organisatoriska åtgärder som styrning, organisation, kommunikation, utbildning och styrdokument. För att erhålla en god motståndskraft mot cyberattacker krävs således ett övergripande, strukturerat och planlagt arbete med informationssäkerhet. Det bör även inkluderas en tydlig plan för hur organisationen ska öka medvetenheten genom planlagda och regelbundna utbildningsinsatser inom informationssäkerhet.

Resultatet av den distribuerade enkäten visar att en stor andel medarbetare inte känner till kommunens riktlinjer om informationssäkerhet och att medvetenheten och kunskapen inom informationssäkerhet samt phishing verkar vara relativt låg. Initialt rekommenderar EY därmed kommunen att se över befintliga riktlinjer kring informationssäkerhet och tillgängligheten för dessa, för att säkerställa att alla medarbetare kan efterleva dem. Vidare rekommenderar EY Lunds kommun att utveckla ett formaliserat utbildningsprogram inom informationssäkerhet för samtliga medarbetare inom kommunen, för att kunna förbättra kommunens motståndskraft mot cyberattacker. Syftet med programmet bör även vara att öka medvetenheten kring vikten av informationssäkerhet, samt att utbilda medarbetare om de hot och risker som finns relaterade till informationssäkerhet i deras dagliga arbete. Programmet rekommenderas att inkludera specifika mål för utbildningar inom informationssäkerhet, exempelvis olika delmål för olika informationssäkerhetsområden. Utöver specifika utbildningstillfällen rekommenderas kommunen att kontinuerligt sprida utbildningsmaterial till sina medarbetare, exempelvis i form av checklistor medarbetarna kan följa vid misstanke av en phishingattack.

EY rekommenderar även att kommunen genomför en utförlig intressentanalys för att identifiera särskilda målgrupper inom kommunen som programmet kan rikta sig till. Dessa målgrupper skulle kunna vara förvaltningar i särskilt hög riskgrupp, med anledning av verksamhetens syfte och känslighetsgraden av informationen som hanteras. Utifrån denna analys rekommenderar EY att programmet ska konkretisera hur kommunikation och utbildningsaktiviteter med respektive målgrupp ska utformas, genomföras och följas upp.

3.2 Teoretiska och praktiska övningar inom phishing

I takt med att mängden cyberattacker mot organisationer har ökat de senaste åren har EY även noterat en markant ökning i antalet phishingattacker. En av anledningarna som EY har sett är COVID-19 och den ökade användningen av digitala verktyg. Anställdas medvetenhet och kunskap om informationssäkerhet blir således allt viktigare för att säkerhetsställa ett adekvat skydd av informationen hos en organisation, samt för att uppfylla gällande lagkrav om informationssäkerhet och dataintegritet. Att klicka på en inbäddad länk i ett e-postmeddelande eller uppge användardata under en pågående cyberattack genom phishing kan leda till stora konsekvenser, både på individ-och organisationsnivå. Detta då cyberkriminella kan försöka utvinna konfidentiell information eller implementera skadlig kod på mottagarens enhet.

Den simulerade attacken visade att 33 procent av mottagarna klickade på länken i e-postmeddelandet och att 19 procent av mottagarna uppgav sin användardata på landningssidan. Resultaten indikerar att kommunen löper en mycket hög risk för att utsättas för en fullbordad phishingattack i jämförelse med de på förhand bestämda acceptansnivåerna. Baserat på detta resultat rekommenderar EY att teoretiska och praktiska övningar inom phishing planeras, schemaläggs och följs upp för alla medarbetare inom kommunen. Syftet med övningarna är att förbättra medvetenheten och kunskapen om phishing genom hela kommunen och specifikt i de delar av kommunen som löper störst risk för denna typ av attacker. Vidare rekommenderar EY även kommunen att satsa på teoretiska övningar för att stärka medarbetarnas förmåga att identifiera falska e-postmeddelanden och förstå vilka konsekvenser en fullbordad phishingattack kan innebära. De här övningarna kan handla om interaktiva diskussioner där medarbetarna får möjlighet att jämföra sofistikerade falska e-postmeddelanden med autentiska e-postmeddelanden och reflektera över skillnaderna.

EY rekommenderar vidare att Lunds kommun följer upp de teoretiska inslagen med praktiska övningar som regelbundna tester av säkerhetsmedvetenheten och kunskapen om phishing hos medarbetarna. Detta för att kontrollera effekten av genomförda utbildningsinsatser och för att fortsätta sprida kunskapen inom kommunen. Praktiska övningar syftar till att testa kunskapen som diskuterades under de teoretiska tillfällena som att identifiera ett falskt e-postmeddelande, avsändare eller domän. Det finns olika tillvägagångssätt en kommun kan använda för att genomföra tester, men EY rekommenderar att Lunds kommun utforskar möjligheten att fortsätta med uppföljande simuleringar av phishingattacker för att samla in analysbara och enhetliga data.

3.3 Tydliggör rapporteringsvägar och kommunicera betydelsen av rapportering

Det finns olika sätt en organisation kan minska effekterna av en pågående cyberattack genom att underlätta identifiering av attacken, förhindra spridningen och effektivt stoppa den. En viktig faktor är att effektiva rapporteringsvägar existerar, och att de anställda är medvetna om hur och när dessa ska användas. Vid phishingattacker kan rapporteringen av ett misstänksamt e-postmeddelande möjliggöra att hotet identifieras och att adekvata skyddsåtgärder kan vidtas inom skälig tid. Att snabbt identifiera och motverka en phishingattack kan således ha stor påverkan på hur skadliga konsekvenser blir, samt

möjligheterna att stoppa den. Rapporteringsvägen bör också utvärderas regelbundet och övervakas av informationssäkerhetsansvariga inom kommunen.

Resultatet av granskningen visar att det finns brister i rutinerna kring rapportering av säkerhetsincidenter vid en phishingattack hos kommunen. Detta då en stor andel av enkätdeltagarna inte vet att de behöver rapportera en sådan säkerhetsincident, hur de ska gå tillväga för att rapportera en säkerhetsincident, eller till vem de ska vända sig till. Baserat på granskningen rekommenderar EY att Lunds kommun ser över sina befintliga rapporteringsvägar, säkerställer att dessa optimeras och fastställs för att de ska bli en etablerad del av verksamheten. EY anser att det inom kommunen bör finnas väletablerade, dokumenterade rapporteringsvägar tillgängliga för samtliga medarbetare för att säkerställa att kommunen kontinuerligt informeras om potentiella eller pågående säkerhetsincidenter relaterade till phishingattacker. Rapporteringsvägarna bör vara tydligt kommunicerade och tillgängliga för alla medarbetare inom kommunen. Om en medarbetare har frågor kring rapporteringsvägar bör det var tydligt var, eller till vem, de ska vända sig för att få stöd i dessa frågor.

Utöver detta rekommenderar EY Lunds kommun att arbeta vidare med att kommunicera vikten av att rapportera eventuella säkerhetsincidenter inom kommunen. Kommunikationen bör inkludera tydliga förväntningar och kravställningar på rapportering hos samtliga medarbetare då man misstänker att man blivit utsatt för en cyberattack eller att man angett användarinformation. EY bedömer att rapporteringsfrekvensen hos en organisation som utsätts för en phishingattack riskerar att minska vid ökat hemarbete, då medarbetare inte har samma regelbundna kontakt med varandra. Denna risk är således ytterligare en faktor som talar för behovet av att kommunicera vikten av att rapportera säkerhetsincidenter till samtliga medarbetare inom kommunen.

4. Revisionsfrågor

Granskningen har utgått från två revisionsfrågor. Hur väl Lunds kommun uppfyller dessa revisionsfrågor beskrivs nedan.

Färgkod	Förklaring
	Revisionsfråga uppfylls ej
	Revisionsfråga uppfylls delvis
	Revisionsfråga uppfylls

Revisionsfråga	Svar	
▶ Hur väl hanterar kommunstyrelsen hotet från attacker genom falska email, så kallad phishing?	Baserat på genomförd granskning bedömer EY att Lunds kommun bör arbeta för att förbättra sin motståndskraft för att kunna stå emot det ökade hotet av phishingattacker. Resultatet av simuleringen indikerar att kommunen löper en mycket hög risk att utsättas för en fullbordad phishingattack i relation till acceptansnivåerna som kommunen tillsammans med EY bestämt. Vidare visar enkäten att en mycket stor andel av medarbetarna saknar kunskap och förståelse kring cyberrisker, samt hur angrepp ska hanteras. Detta styrker behovet av att vidta åtgärder för att utbilda medarbetare, tydliggöra och dokumentera riktlinjer och rutiner kring phishingattacker, samt kommunicera dessa inom organisationen. Därutöver finns mycket stora brister i rutinerna kring incidentrapportering. Slutsatsen är att Lunds kommun ligger på en nivå markant under det man bör förvänta sig av en kommun av denna storlek och karaktär.	

► Kan kommunstyrelsens säkerhetsarbete kopplat till attacker med falska email anses vara ändamålsenligt?	Resultatet av granskningen visar tydligt att det finns ett behov av att förbättra säkerhetsarbetet kopplat till phishingattacker. EY har därför valt att presentera de mest relevanta och övergripande rekommendationerna som kommunen bör fokusera sitt arbete på: ► Utveckla ett strukturerat och regelbundet arbete med utbildning inom informationssäkerhet, särskilt fokuserat på de delar av organisationen med hög risk – exempelvis socialförvaltningen. ► Genomföra både teoretiska samt praktiska övningar inom phishing. ► Vidareutveckla befintliga rapporteringsvägar, dokumentera dessa, samt kommunicera vikten av att rapportera säkerhetsincidenter.	

5. Slutsatser

EY har noterat att antalet cyberattacker har ökat stort under de senaste åren. Bland dessa attacker kan det särskilt noteras en ökning av phishingattacker, vilket innebär att en angripare genom falska e-postmeddelanden försöker lura användare att klicka på skadliga länkar och lämna ut användarinformation. Anställdas medvetenhet och kunskap kring informationssäkerhet blir således allt viktigare för att säkerställa ett adekvat skydd av informationen hos en organisation, samt för att uppfylla gällande lagkrav kring informationssäkerhet och dataintegritet. Att klicka på en inbäddad länk som kan innehålla skadlig kod eller lämna ut användarinformation under en pågående cyberattack kan leda till allvarliga konsekvenser som obehörig tillgång till kommunens information och interna system, manipulation av kommunens tjänster, samt att persondata och känsliga uppgifter läcks ut. Det kan exempelvis räcka att en enda användare uppger sitt användarnamn och lösenord för att cyberkriminella ska få tillgång till sekretessbelagd information vilket kan få förödande konsekvenser.

Den här granskningen syftade till att undersöka det praktiska arbetet med IT- och informationssäkerhet inom Lunds kommun. Genom en simulerad phishingattack har EY testat utbildning och medvetenhet hos personalen. Den genomförda granskningen svarar på följande revisionsfrågor:

- Hur väl hanterar kommunstyrelsen hotet från attacker genom falska email så kallad phishing?
- Kan kommunstyrelsens säkerhetsarbete kopplat till attacker med falska email anses vara ändamålsenligt?

Resultatet från granskningen indikerar att det finns ett behov av att förbättra utbildning och medvetenhet kring IT- och informationssäkerhet. En stor andel medarbetare är inte medvetna om hotet från en phishingattack, samt har inte kunskapen att kunna identifiera ett falskt e-postmeddelande och landningssida. Vidare pekar resultatet från enkäten på att en stor andel av personalen inte är medvetna om kommunens riktlinjer kring informationssäkerhet, eller hur de ska gå tillväga för att rapportera en säkerhetsincident relaterad till e-postattacker. Kommunen rekommenderas därför att vidta åtgärder för att stärka utbildning och medvetenheten hos medarbetarna, samt åtgärda svagheter i motståndskraften mot phishingattacker. Detta för att undvika förluster av känslig information, negativt rykte eller andra betydande konsekvenser.

Baserat på resultatet från granskningen har EY valt att presentera följande tre övergripande rekommendationer som Lunds kommun bör fokusera sitt arbete på framöver:

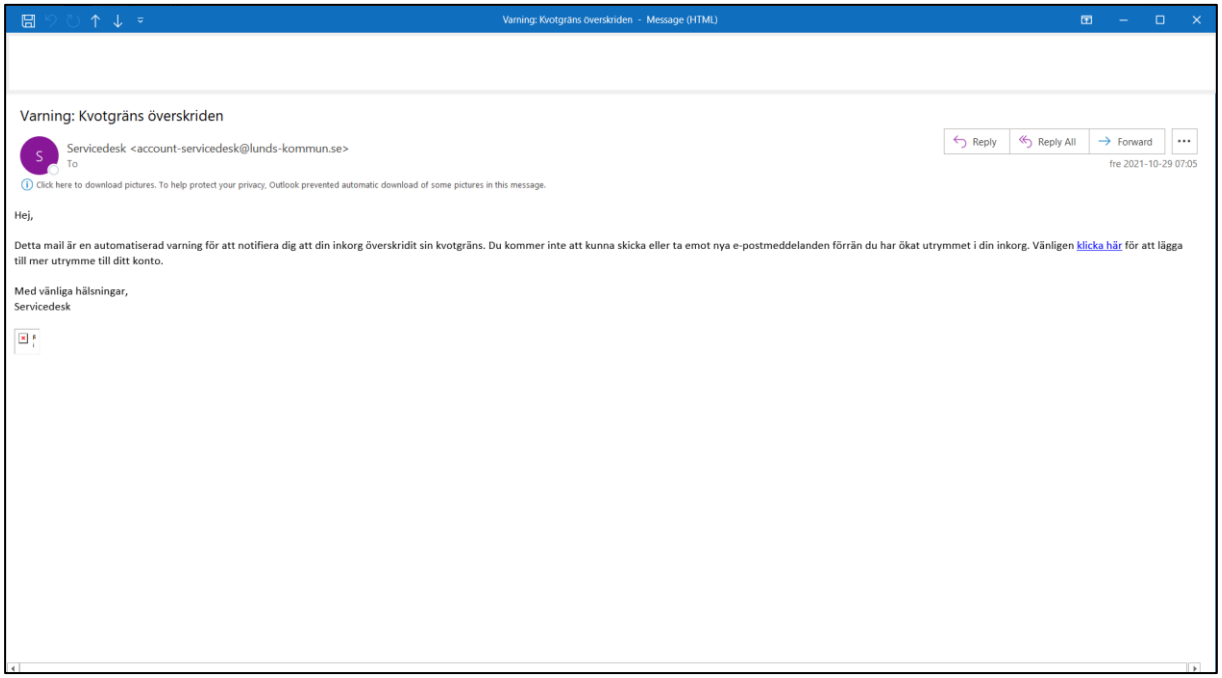
- Utveckla ett strukturerat och regelbundet arbete med utbildningar i informationssäkerhet, särskilt fokuserat på de delar av organisationen som kan vara målgrupper för phishingattacker.
- Genomföra både teoretiska samt praktiska övningar inom phishing.
- Vidareutveckla sina befintliga rapporteringsvägar, säkerställa att dessa är dokumenterade och tillgängliga för alla medarbetare, samt kommunicera vikten av att rapportera säkerhetsincidenter till samtliga medarbetare.

Stockholm 2021-11-29

Helena Törnqvist, Partner, EY

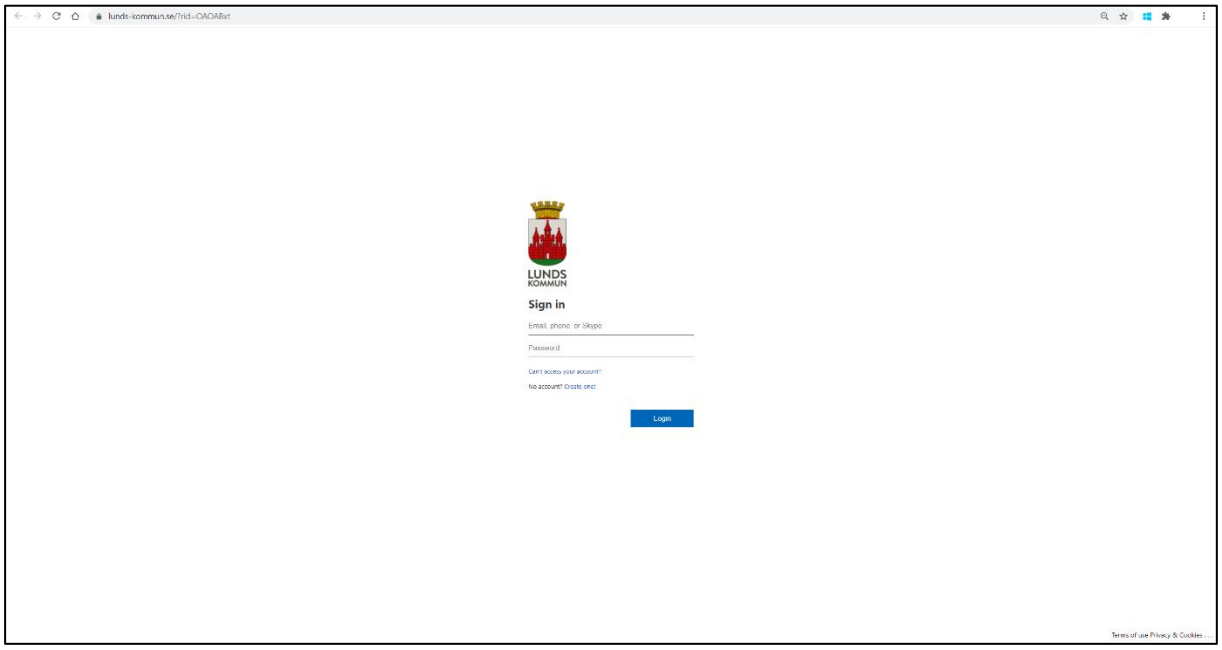
Bilaga 1: E-postmeddelande

E-postmeddelande



Bilaga 2: Landningssida

Landningssida 1



Landningssida 2

OBS! Detta e-postmeddelande var ett phishing-mail.

Det här är en simulation för att stärka motståndskraften inom Lunds kommun för att kunna stå emot cyberattacker genom phishing (svenska: nätfiske).

Denna övning utfördes i samarbete med EY som en del av kommunens fortsatta arbete inom informationssäkerhet. Vi hoppas med den här övningen fortsätta utveckla medvetenheten av potentiella cyberattacker hos oss på kommunen.

Bedrägerier i form av social manipulation som phishing är ett växande problem i samhället, och ett förfalskat e-postmeddelande kan vara svårt att upptäcka. Vänligen se tipsen nedan som hjälp för att i framtiden lyckas känna igen denna typ av e-postmeddelanden på arbetsplatsen och även i privata sammanhang.

Den användarinformation du har angett är anonymiserad och kommer att raderas. Det är endast aggregerad statistik som kommer samlas in.

Vi vill bedöma anställdas grad av försiktighet och medvetenhet om phishing och uppskattar därför om du inte diskuterar detta e-postmeddelande med kollegor eller informerar dem om övningen.

Stanna upp, se efter och tänk till!

Finns det något i e-postmeddelandet som var ovanligt? Bedragare utnyttjar ofta stressiga situationer för att få oss att agera hastigt. Var särskilt kritisk till e-postmeddelanden som uppmanar dig att kringgå vanliga procedurer och/eller agerar snabbt. Är det troligt att du skulle få den här typen av e-postmeddelande utan någon tidigare information från din arbetsgivare?

Om du misstänker att du har utsatts för phishing, kontakta genast servicedesk.

1. Kontrollera avsändare

Om du misstänker att ett e-postmeddelande inte är äkta, tänk på att vara kritisk till innehållet och leta efter saker som inte stämmer. Domänen @lunds-kommun.se från vilken e-postmeddelandet skickades är inte en domän som Lunds kommun använder utan en så kallad bluffdomän. Dessa är gjorda så att man vid första anblick inte ska misstänka att någonting är fel.

2. Kontrollera språket

Håll utkik efter stavfel. Seriösa e-postmeddelanden innehåller oftast inte stavfel och brukar inte vara skrivna på dålig svenska. Men, det är viktigt att förstå att cyberkriminella även kan använda sig av mer sofistikerade metoder. Notera att dessa typer av e-postmeddelanden kan vara välformulerade, som i den här simulerade övningen.

3. Kontrollera länkar

Klicka aldrig på länkar inbäddade i e-postmeddelande om du misstänker att någonting inte stämmer, eller om du inte förväntar dig att få liknande e-postmeddelanden.

Bilaga 3: Acceptansnivåer

	Mycket hög risk	Hög risk	Medel risk	Låg risk
Andel mottagare som klickar på länken i e-postmeddelandet	>15%	10-15%	5-10%	<5%
Andel mottagare som uppger användarinformation på landningssidan	>6%	4-6%	2-4%	<2%

Bilaga 4: Enkätfrågor

Frågor om e-postmeddelandet

1. Vad var anledningen till att du klickade på länken?
    - Jag tycker att e-postmeddelandet såg trovärdigt ut
    - Jag visste inte att det var fel att trycka på en länk i ett e-postmeddelande
    - Jag kände mig stressad att agera
    - Jag klickade inte på länken
    - Annat

2. När insåg du att det här e-postmeddelandet var "phishing"?
    - När jag såg e-postmeddelandet
    - När jag klickat på länken och skickades till landningssidan
    - När jag hade lämnat mina uppgifter och såg informationen om övningen
    - När jag blev varnad om att e-postmeddelandet var falskt, exempelvis från en kollega eller kommunen
    - Annat

3. Rapporterade du e-postmeddelandet?
    - Ja, jag rapporterade till IT-avdelningen
    - Ja, jag rapporterade via en annan rapporteringskanal
    - Nej, men jag kontaktade avsändaren av e-postmeddelandet
    - Nej, jag vet inte hur man rapporterar sådana händelser
    - Nej, jag visste inte att jag skulle rapportera sådana incidenter
    - Nej, då jag insåg att det var en övning såg jag inget behov av att rapportera det
    - Annat

Frågor om säkerhetskulturen

Frågorna om säkerhetskultur delas upp i tre underområden: 1) Utbildning och medvetenhet, 2) Policy och riktlinjer, samt 3) Rapportering. Följande frågor besvaras på en skala enligt nedan:

1. Instämmer helt
2.
3.
4.
5. Instämmer inte alls.

Utbildning och medvetenhet

- Jag får tillräcklig utbildning i informationssäkerhet relaterad till min roll på kommunen
- Jag får kontinuerlig, relevant och tillräcklig information om informationssäkerhet från kommunen
- Jag vet vad en phishingattack är och hur man ska reagera på sådana attacker

Policy och riktlinjer

- Jag känner till kommunens informationssäkerhetspolicy samt relaterade riktlinjer
- Jag tycker att informationssäkerhetspolicyn och relaterade riktlinjer är lätta att förstå och följa
- Jag är medveten om de potentiella hot och negativa konsekvenser som kan uppstå av att inte efterleva kommunens policyer och riktlinjer kring informationssäkerhet.

Rapportering

- Jag förstår vikten av att rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishingattack
- Jag uppmuntras att rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishingattack
- Jag är medveten om hur och till vem jag ska rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishingattack
- Jag känner att jag har gjort något fel när jag rapporterar säkerhetsincidenter orsakade av mig

Bilaga 5: Definitioner

Acceptansnivåer: Acceptansnivåer är ett sätt att översätta generella och övergripande risknivåer till aktuella mätetal som går att följa upp och agera på. Acceptansnivåer bör utgå från organisationens eller företagets kontext, dvs. risknivåer och riskaptit.

Cyberattack: En cyberattack är ett samlingsnamn för olika typer av brott som utförs på IT-system. Attackerna kan utföras för att få tillgång till hemlig information, begränsa tillgången till IT-systemen, samt förstöra data eller IT-system.

Domän: Domän, även kallat domännamn, är en beskrivning av ett namn eller en adress på internet. Vanliga exempel på domännamn är det man skriver in i en webbläsare för att komma till en internetsida eller det som kommer efter "@" i en mailadress, exempelvis "google.com" eller "svt.se".

Falsk avsändare: En falsk avsändare är en avsändare som utger sig för att vara någon den inte är, exempelvis genom att imitera kända e-postadresser eller andra avsändare.

Inbäddad länk: En inbäddad länk är en länk man exempelvis bäddar in i en text eller i en bild, vilket innebär att man kan minska transparensen i att en länk existerar eller vart den leder. Processen är vanlig i phishingattacker då det ökar mottagarnas benägenhet att trycka på länken.

Intranät: Till skillnad från internet som är tillgängligt för alla är ett intranät ofta privat och bara tillgängligt för den organisation eller företag som äger det. Ett intranät är vanligtvis skyddad från omvärlden av en brandvägg och kan bestå av många sammankopplade lokala nätverk.

IT-infrastruktur: IT-infrastruktur är de komponenter inom en organisation som tillsammans används för att producera, hantera, beräkna, hämta och lagra data. Exempel på detta kan vara en databas eller olika servrar.

Landningssida: En landningssida är en internetsida dit en användare hänvisas efter att exempelvis ha tryckt på en länk eller någon annan form av uppmaning.

Phishing: Phishing, på svenska kallat nätfiske, är en metod för cyberkriminella att attackera privatpersoner, företag samt organisationer. Metoden går att utforma på olika sätt men går generellt sätt ut på att lura en mottagare att ladda ner en fil, öppna ett dokument eller trycka på en länk via ett sms eller ett e-postmeddelande. Syftet av phishingattacker är att utvinna konfidentiell information eller att implementera skadlig kod.

Rate limiting: Rate limiting är en engelsk term som beskriver en inbyggd kontroll som existerar i olika e-postklienter, exempelvis Outlook. Kontrollen begränsar antalet e-postmeddelanden som kan tas emot samtidigt för att förhindra en eventuell överbelastning.

Spamfilter: Spamfilter, även kallat skräppostfilter, är en inbyggd kontroll som existerar i olika e-postklienter, exempelvis Outlook. Kontrollen sorterar alla e-postmeddelanden som en mottagare tar emot och filtrerar ut de e-postmeddelanden som troligtvis är skräppost.

Vitlistning: Vitlistning är en metod företag och organisationer använder för att kontrollera e-posttrafiken. Detta genom att på förhand definiera vilka e-postadresser som är godkända (vitlistade) och på så sätt tillåta kommunikationen.