




Södertälje kommun

Rapport: Informationssäkerhet i praktiken
December 2022



Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Södertälje kommun har EY genomfört en granskning för att testa hur väl kommunens arbete med IT- och informationssäkerhet har kommunicerats till medarbetare, exempelvis genom utbildningar och instruktioner. Granskningen syftade till att undersöka om det finns brister i det praktiska arbetet med medarbetarna kring IT- och informationssäkerhet. Detta bedöms genom att simulera ett angrepp via e-post, där kommunens tekniska skydd har kopplats bort. De följande revisionsfrågorna har legat till grund för granskningen:

- ▶ Hanterar Södertälje kommuns medarbetare hotet från attacker genom falska e-postmeddelanden, så kallad phishing (nätfiske), på ett ändamålsenligt sätt?
- ▶ Har Södertälje kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av de testade medarbetarna under den simulerade attacken?
- ▶ Är riktlinjerna för hantering och rapportering av falska e-postmeddelanden och andra incidenter kända hos medarbetarna?

Granskningen genomfördes från september till december 2022. EY utformade och genomförde granskningen tillsammans med representanter från kommunen i syfte att uppnå en så stor nytta som möjligt av resultatet. Metoden som använts bygger på EY:s beprövade metodik för att genomföra en simulerad phishing-attack. Tre huvudområden analyserades: 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 gällande utbildning och medvetenhet inom informationssäkerhet i Södertälje kommun. Granskningsresultatet visar att kommunen ligger på en nivå under det man enligt EY bör förvänta sig av jämförbara organisationer inom den kommunala sektorn. Slutsatsen baseras på den typ av verksamhet som bedrivs och på känslighetsgraden av den information, exempelvis personuppgifter, som behandlas. I relation till acceptansnivåerna löper Södertälje kommun en mycket hög risk att utsättas för en fullbordad phishing-attack. Kommunstyrelsen rekommenderas därför att vidta åtgärder för att informera om relaterade styrdokument och riktlinjer, begränsa antalet rapporteringsvägar för att få en effektiv och samlad rapportering, samt stärka utbildning och medvetenheten hos medarbetarna. En förbättrad motståndskraft mot phishing kan bidra till att förluster av känslig information, negativt rykte eller andra betydande konsekvenser minskar. Baserat på granskningen har EY valt att presentera tre övergripande rekommendationer:

- ▶ Informera om riktlinjer för informationssäkerhet och phishing.
- ▶ Tydliggör och informera om rutiner för rapportering av misstänkta e-postmeddelanden.
- ▶ Inför både teoretiska och praktiska utbildningar inom informationssäkerhet och phishing.

Innehållsförteckning

Sammanfattning	2
Innehållsförteckning	3
1. Bakgrund	4
1.1 <i>Phishing och nätfiske</i>	4
1.2 <i>Syfte och revisionsfrågor</i>	5
1.3 <i>Avgränsningar</i>	5
1.4 <i>Metod och genomförande</i>	5
2. Analys	11
2.1 <i>Mottagare som klickade på länken i e-postmeddelandet</i>	11
2.2 <i>Mottagare som uppgav användarinformation på landningssida</i>	13
2.3 <i>Mottagares medvetenhet kring informationssäkerhet och phishing</i>	15
3. Övergripande rekommendationer	20
3.1 <i>Informera om riktlinjer för informationssäkerhet och phishing</i>	20
3.2 <i>Tydliggör och informera om rutiner för rapportering av misstänkta e-postmeddelanden</i>	20
3.3 <i>Teoretiska och praktiska utbildningar inom phishing</i>	21
4. Revisionsfrågor	23
5. Slutsatser	25
Bilaga 1: E-postmeddelande	26
Bilaga 2: Landningssida	27
Bilaga 3: Acceptansnivåer	29
Bilaga 4: Enkätfrågor	30
Bilaga 5: Enkätresultat	32
Bilaga 6: Definitioner	34

1. Bakgrund

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

Kommunens revisorer har identifierat risker relaterat till kommunens övergripande arbete med IT- och informations säkerhet. Revisorerna har därför valt att genomföra en granskning för att testa hur väl kommunens riktlinjer och rutiner med IT- och informations säkerhet har kommunicerats till medarbetarna i praktiken.

Granskningen genomförs genom att EY simulerar en attack där falska e-postmeddelanden skickas ut till medarbetarna, en så kallad phishing- eller nätfiskeattack. Eftersom det är medarbetarnas motståndskraft som testas har det tekniska skyddet kopplats bort för denna simulering. Genom ett fullgott informations säkerhetsarbete från kommunens sida, bör medarbetarna kunna identifiera ett sådant angrepp, och veta hur de ska agera för att hantera och rapportera den simulerade attacken med bibehållen säkerhet. Med hjälp av resultatet på hur många som agerade korrekt kan revisorerna få en bild av hur medvetna medarbetarna är och hur väl utbildning fungerar i praktiken.

1.1 Phishing och nätfiske

Ökad digitalisering leder till ökade informations säkerhetsrisker. Cyberkriminella attackerar inte enbart en organisations tekniska miljö utan väljer i hög utsträckning att rikta in sig på människorna i organisationen. Cyberkriminella ägnar sig åt social manipulation genom att utnyttja mänskliga svagheter såsom rädsla och förtroende för att komma åt känslig information eller för att sprida skadlig kod, något som riskerar att allvarligt skada organisationer, deras intressenter och samhället i stort. Under covid-19-pandemin har EY sett en ökning av denna typ av cyberkriminalitet, särskilt genom phishing. Det är svårt att fullt ut skydda en organisation mot phishing-attacker enbart genom tekniska hjälpmedel. Detta innebär att den mänskliga aspekten blir avgörande för att säkerställa ett adekvat skydd av en organisations tillgångar och för att uppfylla lagkrav om informations säkerhet och integritet.

En fullbordad phishing-attack kan innebära stora konsekvenser för en organisation, både ekonomiskt och i form av försämrat anseende och rykte. Det är därmed viktigt att vara proaktiv för att hantera det ökade hotet från phishing. Ett viktigt tillvägagångssätt för detta är att hålla medarbetare inom en organisation medvetna om hotet från phishing, och ge dem kunskapen att kunna identifiera falska e-postmeddelanden. Medarbetare bör även ha en tydlig rapporteringsväg att följa för att rapportera misstänkta e-postmeddelanden. Ett annat sätt att minska riskerna för den här typen av cyberattacker är att kontinuerligt genomföra medvetenhetsträning inom informations säkerhet. Detta för att medarbetare ska kunna upptäcka och reagera på försök till nätfiske.

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 kommunens medarbetare. Vidare är syftet också att bedöma i vilken utsträckning en angripare riskerar att komma åt kommunens IT-miljöer genom angrepp via e-postmeddelanden. De följande revisionsfrågorna har legat till grund för granskningen:

- ▶ Hanterar Södertälje kommuns medarbetare hotet från attacker genom falska e-postmeddelanden, så kallad phishing (nätfiske), på ett ändamålsenligt sätt?
- ▶ Har Södertälje kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av de testade medarbetarna under den simulerade attacken?
- ▶ Är riktlinjerna för hantering och rapportering av falska e-postmeddelanden och andra incidenter kända hos medarbetarna?

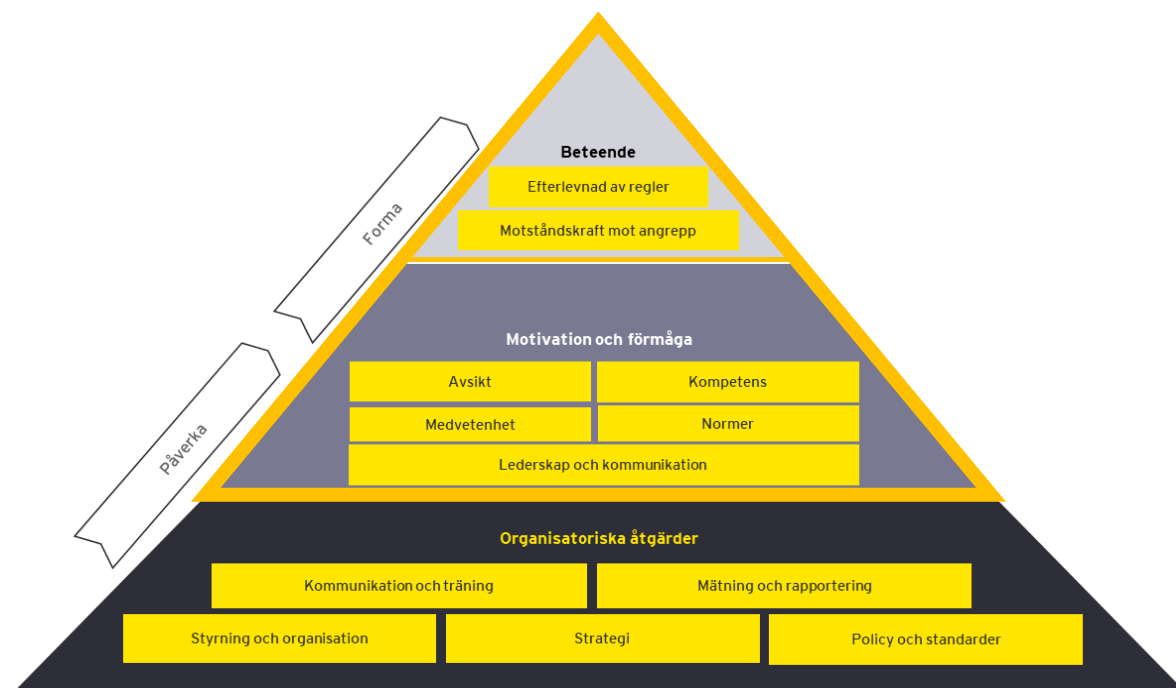
1.3 Avgränsningar

Granskningen är avgränsad till att ge en bild av hur sårbar kommunen är för attacker riktade mot medarbetarna via e-postmeddelanden. Det ges alltså inte någon helhetsbild av kommunens fullständiga arbete inom IT- och informationssäkerhet utan syftet är ge en mer detaljerad bild av ett begränsat område. Ingen teknisk testning har utförts för att granska effektiviteten i kommunens skalskydd, det vill säga hur väl tekniska hjälpmedel 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 att agera i enlighet med de riktlinjer organisationen fastställt. 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 medarbetarna i Södertälje kommun har i denna granskning utvärderats genom en enkät som distribuerades efter genomförd övning. Enkätens syfte var även att mottagarna själva skulle reflektera över deras medvetenhet, kunskap och beteende kring informationssäkerhet.

Motivationen och förmågan hos medarbetare 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 medarbetare i Södertälje kommun har i denna granskning utvärderats genom att utföra en simulerad phishing-attack. 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 informations säkerhet

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

1.4.1 Metod

EY använder en beprövad metodik för att genomföra och analysera en simulerad phishing-attack. 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 hur mottagarna hanterat meddelandet. Insamlad information jämförs sedan mot på förhand definierade acceptansnivåer och 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 från IT-avdelningen i Södertälje kommun.

För att besvara revisionsfrågorna har EY analyserat 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.
- ▶ **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 uppgive 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.

- ▶ **Mottagares medvetenhet om 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. En tidig rapportering av ett misstänksamt e-postmeddelande tillåter en organisation att omedelbart upptäcka en cyberattack av detta slag, utreda dess omfattning, samt sätta in lämpliga skyddsåtgärder. EY har därför även undersökt hur många mottagare av det förfalskade e-postmeddelandet att rapportera meddelandet. 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.

1.4.2 Genomförande

Övningen har utformats och genomförts av specialister inom IT- och informationssäkerhet från EY, tillsammans med utvalda representanter från Södertälje 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 phishing-attack 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 medarbetarna 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. Det aktuella meddelandet uppgavs vara skickat från kommunens ekonomiavdelning, men skickades från en e-postadress med domänen "sodertaljekomun.se", vilket är en domän som inte tillhör Södertälje kommun. I e-postmeddelandet uppmanades mottagaren att klicka på en länk för att betala öppnade fakturor. Genom att följa länken i e-postmeddelandet landade besökaren på den förfalskade landningssidan där de ombads logga in med sitt Microsoft 365-konto (e-

postadress och lösenord). Om en mottagare valde att fylla i sina användaruppgifter på landningssidan, skickades de vidare till ytterligare en landningssida som informerade mottagaren att de deltagit i en simulerad phishing-attack. Syftet med den informerande landningssidan är att skapa medvetenhet om informationssäkerhet i organisationen och informera om 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 phishing-attack 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 medarbetarnas medvetenhet.

I samråd med kommunens representanter beslutades det att ett urval på cirka 15 procent av kommunens medarbetare skulle delta i simuleringen. I urvalet exkluderades timvikarier, konsulter och elever, vilket skulle kunna påverka återspeglingsgraden av resultatet inom kontoren med mindre andel ordinarie personal. Det här urvalet baserades även på servicedesks förmåga att hantera inkommande ärenden. Detta resulterade i att 912 medarbetare deltog i övningen.

Kommunens servicedesk sköts av en leverantör och det bör särskilt noteras att överenskommelsen med leverantören begränsar möjligheten till att testa samtliga användare. I detta fall uppgav servicedesk att de har en gräns på att hantera maximalt 20 ärenden över normal belastning under en dag. Då en simulering med samtliga användare riskerar att generera fler ärenden än så under en och samma dag fick ett urval göras och utskicken spridas ut över flera dagar. Detta får som konsekvens att färre medarbetare får ta del av övningen och att granskningens tillförlitlighet sjunker något. Dock bedöms tillförlitligheten i granskningen fortfarande vara fullt tillräcklig för att dra relevanta slutsatser för revisionen.

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 limiting¹. Detta innebär att kommunens tekniska skydd kopplas bort, i syfte att på ett kostnadseffektivt sätt testa personalen och inte tekniken. Det bör noteras att inget tekniskt skydd fullständigt kan förhindra ett angrepp via phishing. EY genomförde simuleringen den 4 oktober 2022, och bestämde i samråd med kommunen att jämt fördela utskicken av e-post under simuleringens aktiva dagar, i syfte att inte överbelasta servicedesk. Simuleringen var aktiv under vecka 40.

1.4.2.3 Rapportering

Att skydda sig mot hotet från en phishing-attack kan vara svårt och kräver en fungerande samverkan mellan flera olika faktorer. En viktig komponent är att effektiva

¹ För förklaring av begreppen, se definitioner i *bilaga 5*.

rapporteringsvägar existerar och att medarbetarna är medvetna om hur dessa ska användas. 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 misstänker att de blivit utsatta för angrepp vidtar nödvändiga åtgärder för att ändra inloggningsuppgifter som en angripare kan ha fått tillgång till.

Södertälje kommun publicerar varningar och nyhetsnotiser på intranätet som varnar medarbetare för phishing-attacker. På intranätet finns även information som hjälper medarbetarna att kontrollera om ett meddelande är falskt. Om man misstänker att man blivit utsatt för phishing uppmanas medarbetarna att stänga av datorn, felanmäla omgående via telefon och att inte starta om datorn. Vid ett misstänkt falskt e-postmeddelande uppmanas man att rapportera till kommunens servicedesk, antingen genom att ringa eller skicka e-postmeddelande. Det uppmanas även att verifiera misstänksamma filer genom att ta kontakt med avsändaren och/eller informera IT-säkerhetsavdelningen eller servicedesk (via en e-postadress som skickas till Telge). Vidare följer IT-chefen rutinen att vid uppmärksammat phishing be servicedesk att stoppa inflödet av liknande e-postmeddelande till kommunens samtliga e-postkonton, spärra eventuella länkade sidor samt gå igenom alla maillådor för att ta bort liknande e-postmeddelanden.

1.4.2.4 Enkät

Efter avslutad simulering distribuerades ett antal enkätfrågor via kommunen till mottagarna av e-postmeddelandet. Enkäten utformades av EY och syftet var att skapa en förståelse för motivationen och förmågan hos kommunens anställda att identifiera ett falskt e-postmeddelande. Därutöver var syftet även att undersöka om medarbetarna känner till befintliga riktlinjer, utbildningsmöjligheter och rapporteringsvägar. 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 phishing-attack 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 riskerna för vissa förvaltningar kan vara mindre än för andra beroende på typen av verksamhet. Se *tabell 1* för definitioner av risknivåer som EY har använt under genomförd granskning.

Tabell 1: Risknivåer för phishing-övning

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

Innan en simulerad phishing-attack påbörjas är det viktigt att översätta de olika risknivåerna till specifika måttal anpassade för den aktuella organisationen, vilket kallas för acceptansnivåer. 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 2022 till december 2022, se *tabell 2* nedan för granskningens tidsplan.

Tabell 2: Tidsplan

Förberedelser och planering	September 2022
Test och utskick	September - oktober 2022
Rapportskrivning och intern kvalitetssäkring	Oktober 2022
Justering och färdigställande av rapport	November 2022
Avrapportering och slutpresentation	December 2022

2. Analys

En phishing-attack 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. Phishing-attackens 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, och 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. Södertälje kommun hade i samråd med EY på förhand bestämt acceptansnivåer baserat på omfattningen av kommunens informationshantering och riskaptit. *Tabell 3* nedan beskriver de beslutade acceptansnivåerna för andelen mottagare som klickar på länken.

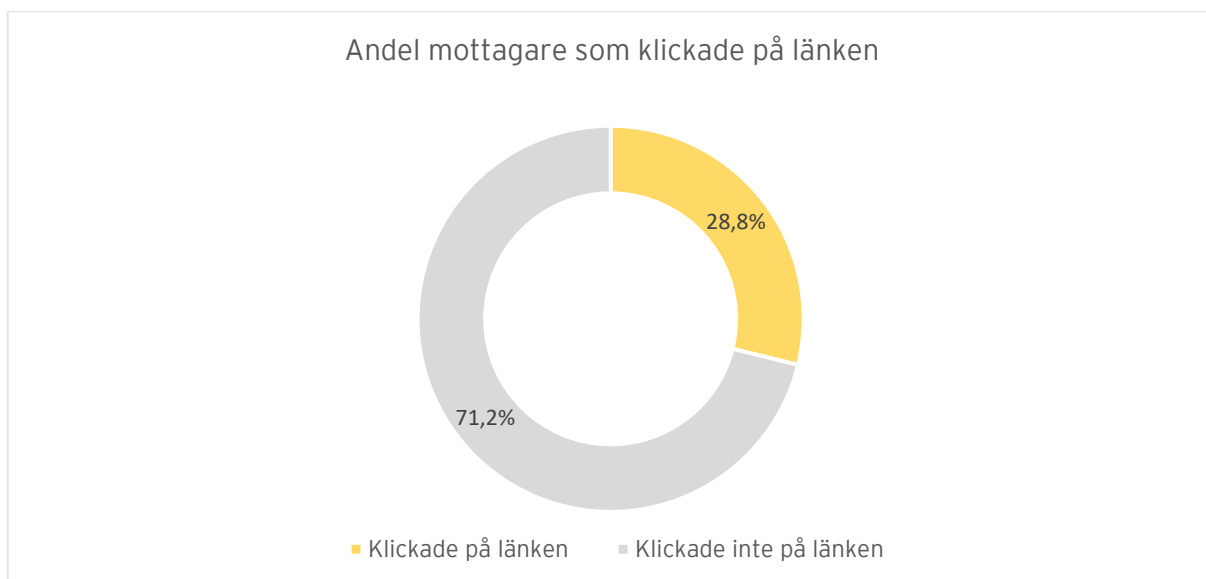
Resultatet av den simulerade attacken för kommunen som helhet visar att 28,8 procent av mottagarna klickade på den inbäddade länken i e-postmeddelandet. Resultatet av granskningen visar att enligt de definierade acceptansnivåerna löper Södertälje kommun en mycket hög risk att utsättas för phishing-attacker.

Tabell 3: Acceptansnivåer för andelen mottagare som klickar på länken

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

2.1.1 Resultat av simulering

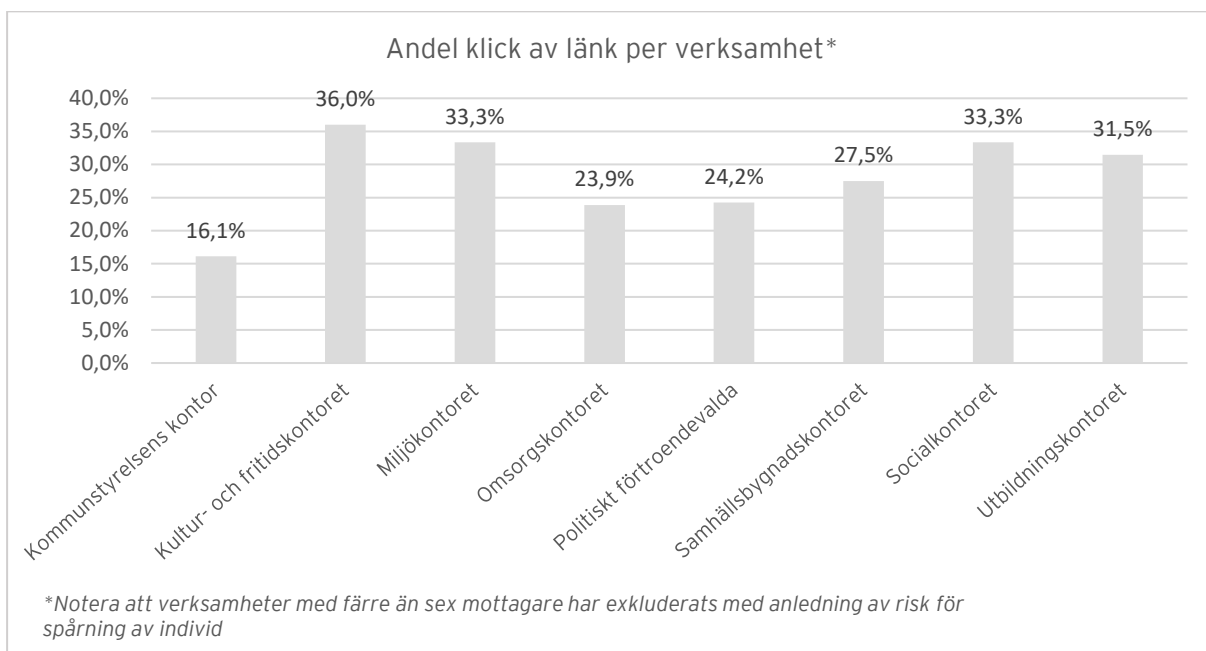
Det insamlade resultatet analyserade hur många mottagare som klickat på länken i det förfälskade meddelandet, dels för kommunen som helhet men även uppdelat på kommunens verksamheter. Av 912 mottagare klickade 263 på länken i e-postmeddelandet, vilket motsvarar 28,8 procent av mottagarna, se *figur 2* nedan. Det här resultatet innebär enligt acceptansnivåerna att Södertälje kommun löper en mycket hög risk för att utsättas för en fullbordad phishing-attack.



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

Simuleringen var aktiv under vecka 40 och utskicket av e-postmeddelanden beslutades i samråd med kommunen att fördelas under flera dagar. EY noterar endast en marginell variation i antal klick per dag och konstaterar därmed en jämn trend. Denna trend är enligt EY förväntad i en simulerad attack då den påkallar omedelbara handlingar av mottagaren och beror på att e-postmeddelandet skickades ut i omgångar. Vid ett verkligt angrepp hade troligtvis antal klick per dag minskat då kommunen enligt rutin ska varna om en pågående phishing-attack.

Figur 3 visar andelen klick på länken i e-postmeddelandet per verksamhet. EY noterar att andelen klick per verksamhetsområde generellt är på en hög nivå i jämförelse med de på förhand bestämda acceptansnivåerna. EY noterar vidare att Kultur- och fritidskontoret hade den högsta andelen mottagare som klickat på länken. Vidare noterat EY att Miljökontoret och Socialkontoret också sticker ut med 33,3 procent vardera av mottagare som klickat på länken. Lägst andel mottagare som klickat på länken hade Kommunstyrelsekontoret. Enligt de bestämda acceptansnivåerna löper följande verksamheter en mycket hög risk att utsättas för en fullbordad phishing-attack.



Figur 3: Fördelning av mottagare som klickade på länken per verksamhet (%). Notera att andel mottagare som klickat på e-postmeddelandet baseras på antalet e-postmeddelanden som skickades till respektive verksamhet.

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 och lösenord på landningssidan. Södertäljes kommun hade i samråd med EY på förhand bestämt acceptansnivåer baserat på verksamhetens omfattning. *Tabell 4* beskriver de beslutade acceptansnivåerna för andelen mottagare som uppgav användarinformation.

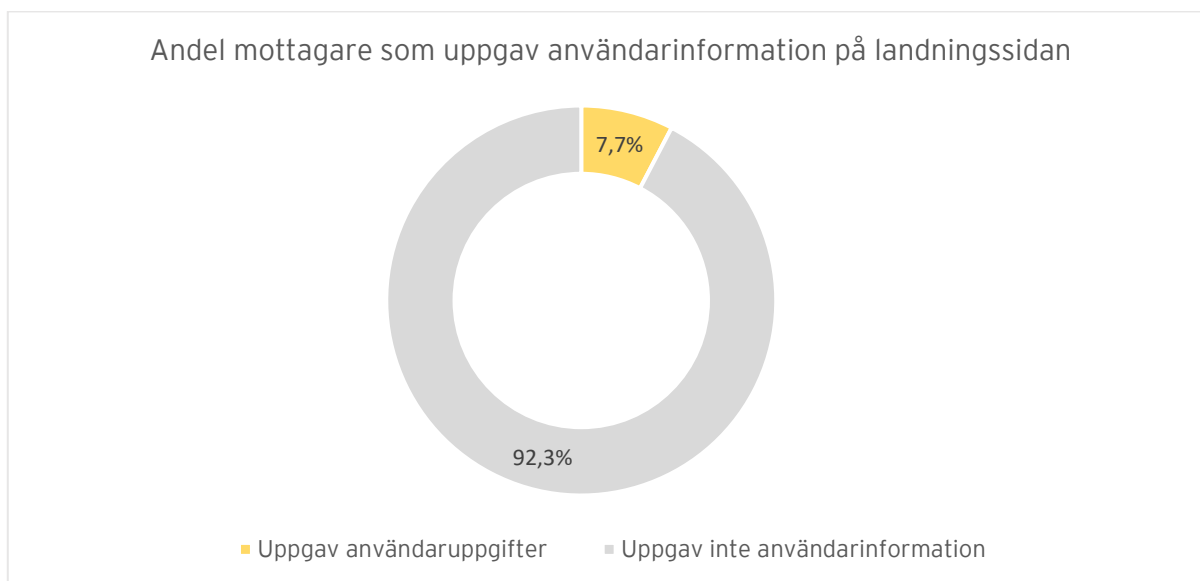
Resultatet av den simulerade attacken för kommunen som helhet visar att 7,7 procent av alla mottagare uppgav sin användarinformation på den förfalskade landningssidan. I relation till de på förhand definierade acceptansnivåerna indikerar resultatet att Södertälje kommun löper en mycket hög risk att utsättas för en fullbordad phishing-attack. 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 en fullbordad phishing-attack är högre om en cyberkriminell får tillgång till användardata och därmed potentiellt kommunens IT-miljöer.

Tabell 4: Acceptansnivåer för mottagare som uppgav användarinformation på landningssidan

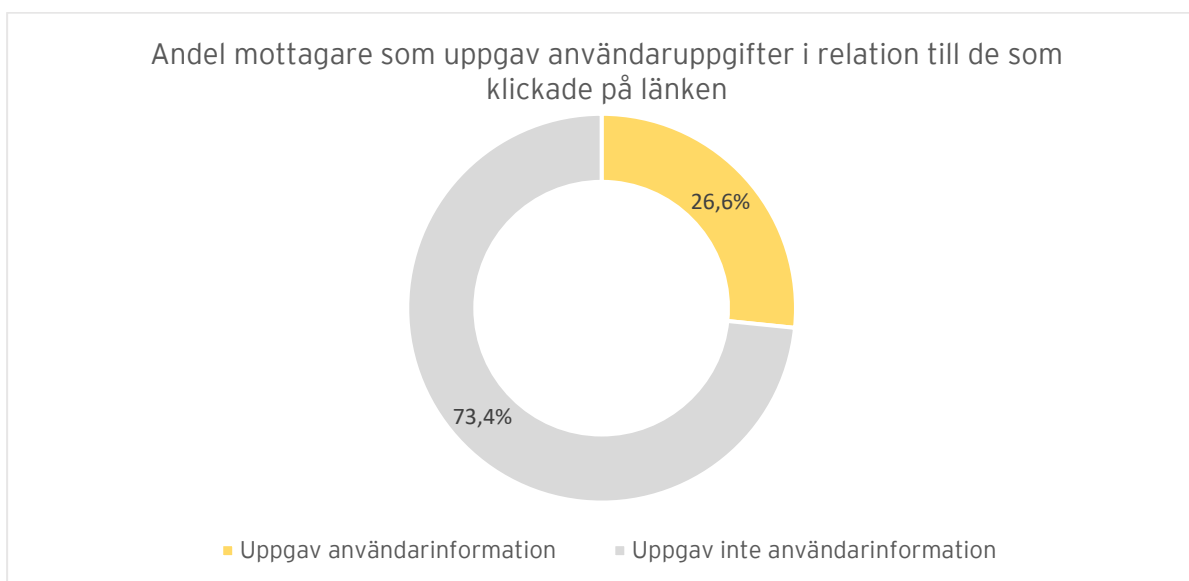
Riskanalys	Acceptansnivå (%)
Mycket hög risk	>6%
Hög risk	4-6%
Medel risk	2-4%
Låg risk	<2%

2.2.1 Resultat av simulering

Av det totala antalet mottagare (912), klickade 70 medarbetare på länken samt uppgav sin användarinformation i form av användarnamn och lösenord på landningssidan. Det motsvarar 7,7 procent av alla mottagare, se *figur 4*. I jämförelse med acceptansnivåerna i *tabell 4*, löper därmed Södertäljes kommun som helhet en mycket hög risk att utsättas för en fullbordad phishing-attack. Då 70 av de 263 medarbetare som klickade på länken även uppgav användarinformation, noterar EY att 26,6 procent av de som klickade på länken valde att uppgive användarinformation medan resterande lämnade landningssidan (*figur 5*).

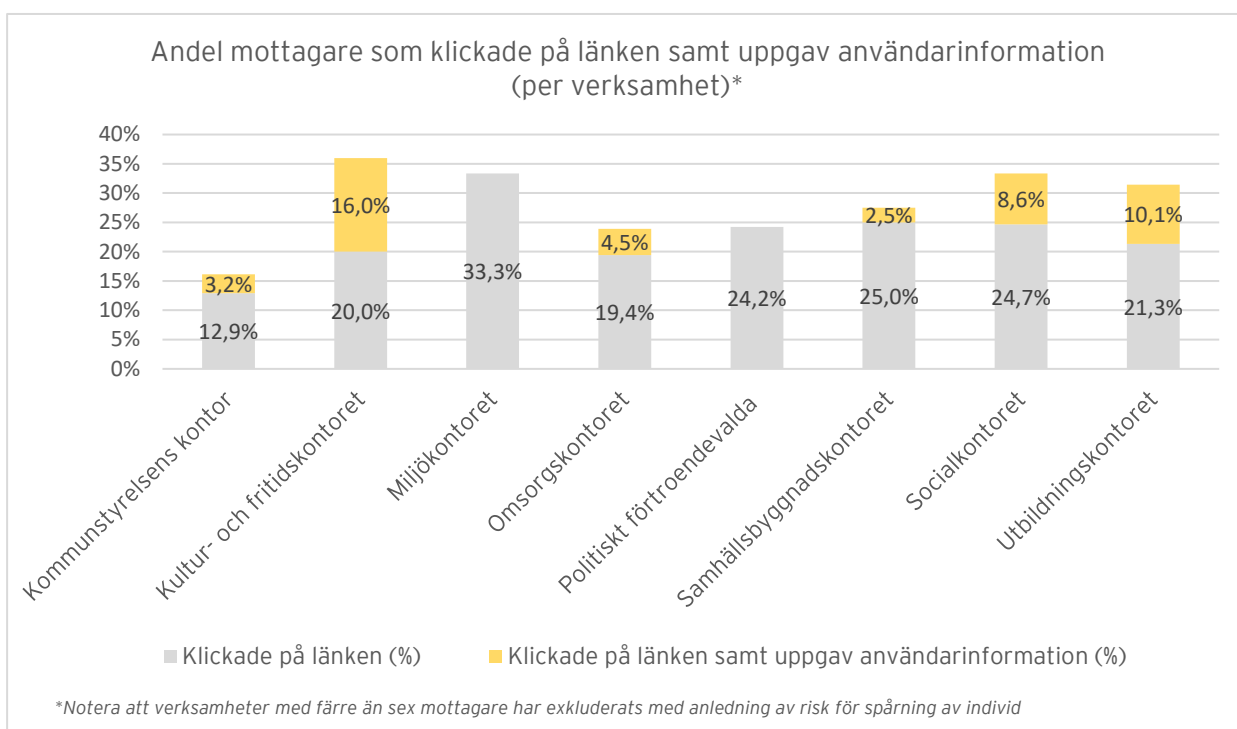


Figur 4: Fördelningen av andel mottagare som uppgav användarinformation på landningssidan (%). Resultatet inkluderar kommunen som helhet, dvs. inkluderat verksamheterna.



Figur 5: Fördelningen av andel mottagare som uppgav användarinformation på landningssidan i relation till de mottagare som enbart klickade på länken. Resultatet inkluderar kommunen som helhet, dvs. inkluderat verksamheterna.

Figur 6 visar andelen mottagare som klickade på länken i e-postmeddelandet i relation till andelen mottagare som utöver att klicka på länken även uppgav användarinformation på landningssidan. Som tidigare noterat var Kultur- och fritidskontoret det kontor där flest mottagare procentuellt klickade på länken. Samma kontor hade även högst andel mottagare som lämnade användarinformation på landningssidan (16 procent), detta följt av Utbildningskontoret och Socialkontoret. Dessa hade ett resultat på 10,1 procent respektive 8,6 procent. Bland de som klickade på länken från Miljökontoret och de politiskt förtroendevalda var det ingen som uppgav användarnamn och lösenord. Baserat på acceptansnivåerna noterar EY att verksamheternas risk varierar. Riskerna att utsättas för en fullbordad phishing-attack bedöms vara antingen mycket hög eller medelhög, med undantag för Miljökontoret och de politiskt förtroendevalda. EY vill även betona att vid en verklig attack kan det räcka med att endast en användare uppger användarinformation för att aktören ska kunna ta sig in i och, i värsta fall, ta kontroll över kommunens IT-miljöer.



Figur 6: Andelen mottagare som klickade på länken i relation till mottagare som först klickade på länken och sedan lämnade användarinformation per verksamhet (%). Notera att andelen mottagare baseras på antalet e-postmeddelande som skickades till respektive verksamhet.

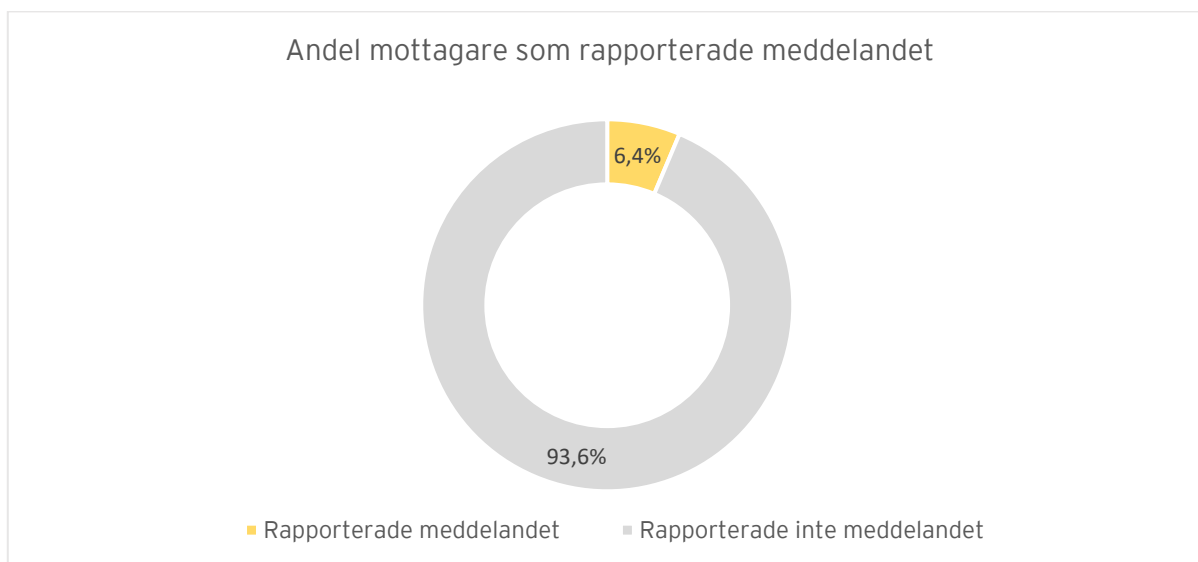
2.3 Mottagares medvetenhet kring informationssäkerhet och phishing

I detta avsnitt presenteras resultatet av andelen medarbetare som identifierade och misstänkte det förfalskade e-postmeddelandet och som valde att rapportera till kommunen. Avsnittet presenterar även resultatet av den enkät som distribuerades efter avslutad simulering. Syftet med enkäten var att skapa en övergripande förståelse för hur medvetna anställda i Södertälje kommun är kring informationssäkerhet och phishing.

Enkäten inkluderade frågor inom följande två områden: 1) E-postmeddelandet som användes i övningen och vanliga indikatorer på phishing, 2) Säkerhetskulturen på kommunen i form av utbildning och medvetenhet, styrande dokument och rapportering av säkerhetsincidenter. Enkäten skickades ut till samtliga deltagare, varav 256 av dessa mottagare deltog i enkätundersökningen. Notera att i denna analys presenteras ett urval av enkätresultatet (se *bilaga 4* och *5* för den fullständiga enkäten).

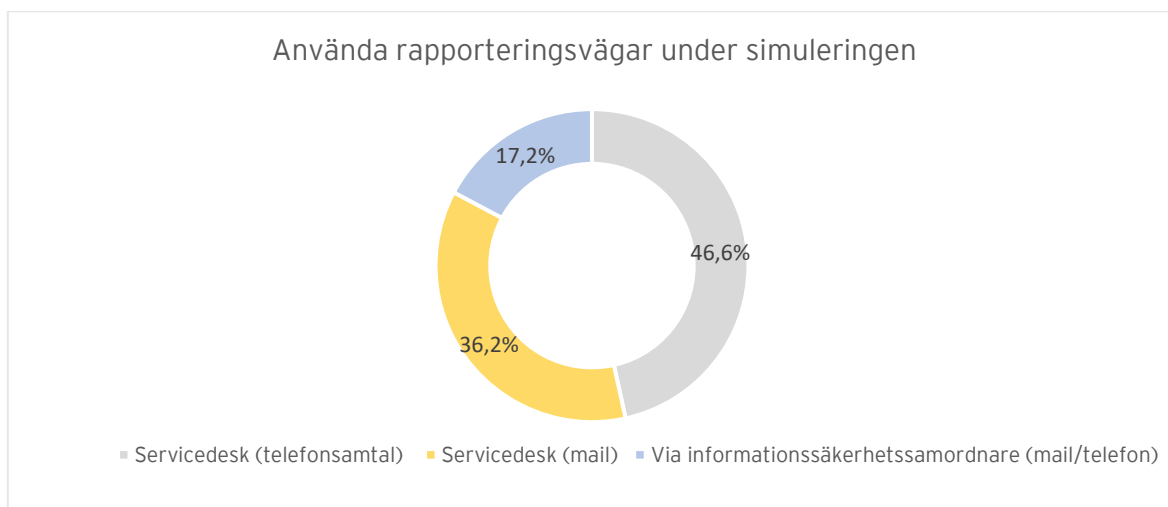
2.3.1 Rapportering

I Södertälje kommun ska misstänksamma e-postmeddelanden rapporteras till kommunens servicedesk. Totalt rapporterade 58 medarbetare e-postmeddelandet under pågående simulering, motsvarande 6,4 procent av alla mottagare, se *figur 7*.



Figur 7: Andel mottagare som rapporterade meddelandet

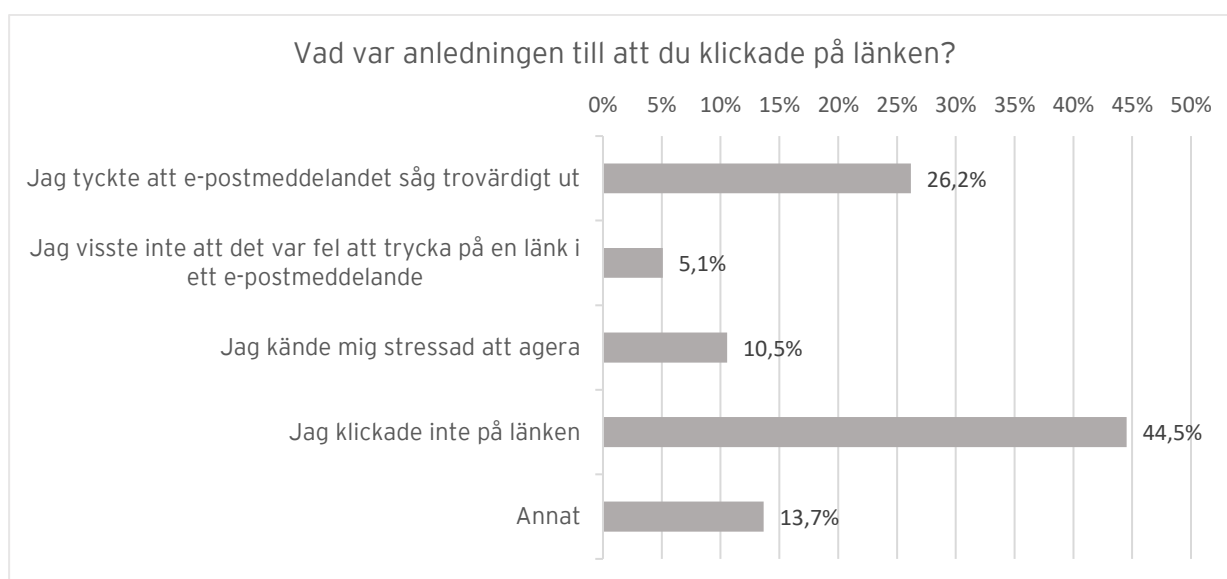
Rapporteringarna inkom genom olika rapporteringsvägar. *Figur 8* nedan visar att den mest frekvent använda rapporteringsvägen var kommunens servicedesk, där 46,6 procent av medarbetare som rapporterade e-postmeddelandet gjorde detta via telefon. Vidare kontaktade 36,2 procent av medarbetarna servicedesk via e-post. Medarbetare valde även att direkt kontakta kommunens informationssäkerhetssamordnare och vid ett tillfälle även IT-chefen för att varna om e-postmeddelandet.



Figur 8: Fördelning av använda rapporteringsvägar under pågående simulering (%).

2.3.2 Resultat av enkät

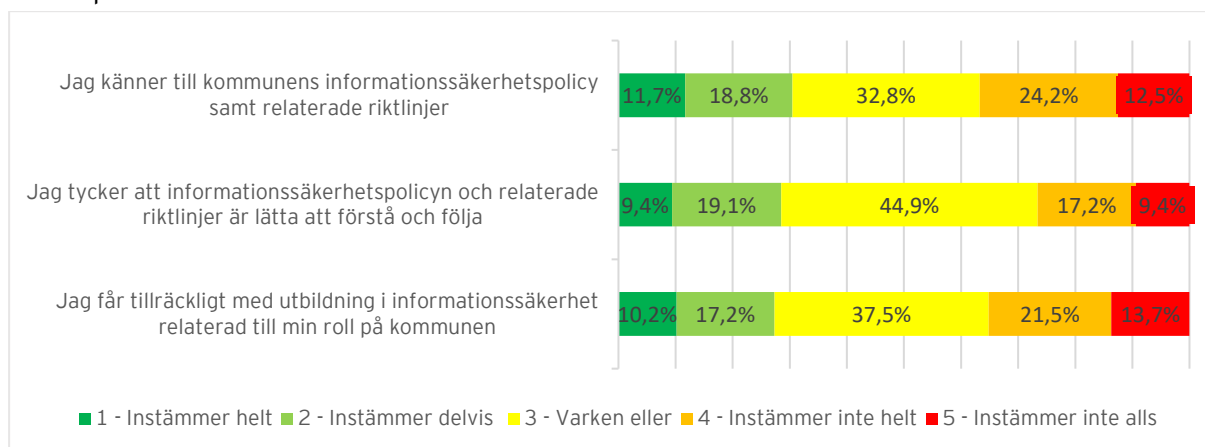
Medarbetares förmåga att identifiera ett falskt e-postmeddelande är av stor vikt för att Södertälje kommun ska kunna minimera riskerna för en fullbordad phishing-attack. *Figur 9* visar olika anledningar till att mottagarna av e-postmeddelandet klickade på den inbäddade länken i e-postmeddelandet. Av de som uppgav att de klickade på länken svarade flest att de tyckte att e-postmeddelandet såg trovärdigt ut, motsvarande 26,2 procent av alla svarande. 10,5 procent av deltagarna uppgav att de klickade på länken för att de upplevde en stress att agera i enlighet med e-postmeddelandets uppmaning. Samtidigt uppgav 13,7 procent av mottagarna andra anledningar till att de klickade på länken. Det handlade bland annat om medarbetare som var stressade och väntade sig få e-postmeddelande om fakturor. Det handlade även om nyfikna medarbetare som insåg att något inte stämde men ändå ville undersöka meddelandet.



Figur 9: Resultat av enkätfråga om länken i e-postmeddelandet (%).

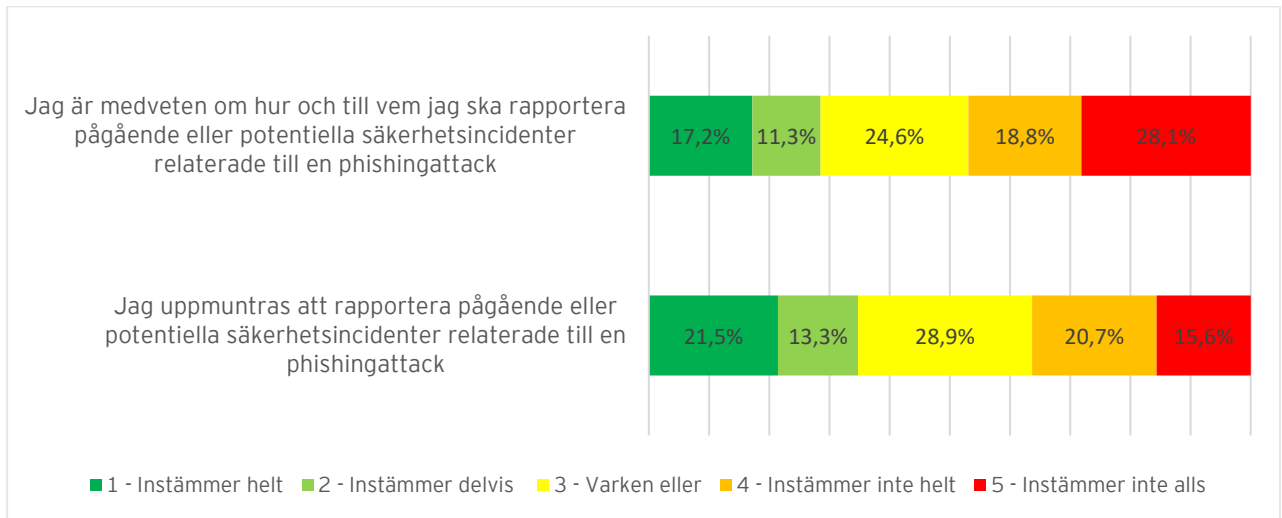
Enkätresultatet visade att 11,7 procent av deltagarna instämmer helt till påståendet att de känner till kommunens nuvarande informationssäkerhetspolicy och relaterade riktlinjer. Den största andelen av deltagarna anger "varken eller" till samma påstående (32,8 procent), samtidigt som 12,5 procent av deltagarna inte alls instämmer att de känner till kommunens informationssäkerhetspolicy. När det kommer till huruvida informationssäkerhetspolicy och relaterade riktlinjer är lätta att förstå och följa uppger 44,9 procent av enkätdeltagarna varken eller. 9,4 procent av enkätdeltagarna väljer svarsalternativet "Instämmer helt" eller "instämmer inte alls".

Den största andelen av enkätdeltagarna (37,5 procent) uppgav varken eller gällande påståendet att de får tillräcklig utbildning inom informationssäkerhet relaterat till deras tjänst på kommunen. 10,2 procent av deltagarna instämmer helt i att de får tillräcklig utbildning inom informationssäkerhet, medan 13,7 procent av deltagarna inte alls anser sig få tillräcklig utbildning inom området. Se *figur 10* för det fullständiga resultatet för dessa påståenden.



Figur 10: Resultat av påståenden om styrande dokument och utbildning inom informationssäkerhet på kommunen (%).

Enkätresultatet indikerar att det råder en viss oklarhet hos enkätdeltagarna kring kommunens rapporteringsrutiner vid säkerhetsincidenter relaterade till en phishing-attack. EY noterar att 28,1 procent av deltagarna anser att de inte vet hur de ska gå tillväga och vem de ska kontakta för att rapportera en pågående phishing-attack. Samtidigt uppger 17,2 procent av enkätdeltagarna att de känner till hur och till vem de ska rapportera en pågående phishing-attack, medan 24,6 procent svarar "varken eller". I relation till detta uppgav 15,6 procent av deltagarna att de inte alls instämmer till påståendet att de uppmuntras av kommunen att rapportera potentiella eller pågående säkerhetsincidenter. Samtidigt instämmer 21,5 procent av deltagarna helt till detta påstående. 28,9 procent av deltagarna svarar "varken eller". Se *figur 11* för det fullständiga resultatet för dessa påståenden.



Figur 11: Resultat av påståenden om phishing-attacker och rapportering (%).

3. Övergripande rekommendationer

Baserat på den genomförda analysen bedömer EY att Södertälje kommun ligger på en nivå under det man bör förvänta sig av jämförbara organisationer inom den kommunala sektorn. Bedömningen baseras på den typ av verksamhet som bedrivs och på känslighetsgraden av den information, exempelvis personuppgifter, som behandlas i den dagliga verksamheten. Således rekommenderar EY att man inom kommunen vidtar åtgärder för att stärka graden av utbildning och medvetenhet hos medarbetarna och därmed stärker motståndskraften mot phishing-attacker. 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 relevanta för Södertälje kommun.

3.1 Informera om riktlinjer för informationssäkerhet och phishing

Enligt EY:s ramverk för hur en organisation arbetar med informationssäkerhet styrs en organisations motståndskraft av dess medarbetares motivation och förmågor. Motivation och förmågor formas av olika organisatoriska åtgärder såsom styrning, organisation, kommunikation, utbildning och styrdokument. För att erhålla en god motståndskraft mot cyberattacker krävs således ett övergripande, strukturerat och planlagt arbete med informationssäkerhet.

36 procent av medarbetarna uppgav i enkäten att de inte känner till kommunens informationssäkerhetspolicy och relaterade riktlinjer, samtidigt som nästan en tredjedel svarade varken eller. Enkäten påvisade även att många medarbetare inom kommunen tycker att kommunens styrdokument är relativt svåra att förstå. Resultatet tyder på att medarbetarnas kännedom om hur kommunen arbetar med informationssäkerhet och phishing är relativt låg, vilket EY även bedömer avspeglar sig i resultatet av den simulerade phishing-attacken då omkring 28 procent av medarbetare klickade på länken i e-postmeddelandet.

Under de inledande mötena med kontaktpersoner från kommunen informerades EY om att det finns dokumenterade riktlinjer för hur medarbetare ska hantera ett förmodat falskt e-postmeddelande vid en phishing-attack. EY fick ta del av dokumentationen och konstaterar att informationen finns att hitta på intranätet. För att stärka arbetet med informationssäkerhet och phishing inom kommunen rekommenderar EY att styrdokument och riktlinjer tydligt kommuniceras till medarbetarna. EY rekommenderar vidare kommunstyrelsen att anordna utbildningstillfällen om innehållet i styrdokument och riktlinjer för att effektivt nå ut till medarbetarna.

3.2 Tydliggör och informera om rutiner för rapportering av misstänkta e-postmeddelanden

En organisation kan minska effekterna av en pågående cyberattack genom att underlätta identifiering av attacken, förhindra spridningen och effektivt stoppa den. En förutsättning för att minimera konsekvenserna av en attack är att effektiva rapporteringsvägar existerar och att medarbetare är medvetna om hur och när dessa ska användas. Rapportering av ett

misstänksamt e-postmeddelande kan möjliggöra att hotet identifieras och att skyddsåtgärder kan vidtas inom skälig tid.

Under de inledande mötena med kommunens kontaktpersoner informerades EY om att servicedesk ska kontaktas vid en incident. Utöver detta finns det information på intranätet som uppmanar medarbetarna att de kan kontakta antingen IT-säkerhetsavdelningen eller servicedesk vid ett misstänkt e-postmeddelande. Resultatet av granskningen indikerar att medarbetarnas medvetenhet av rapporteringsvägar för säkerhetsincidenter relaterade till phishing varierar. 28 procent av enkättagarna uppgav att de inte var medvetna om hur de ska gå till väga och vem de ska kontakta för att rapportera en pågående phishing-attack. Samtidigt uppgav enbart 17 procent att de vet hur de ska rapportera en pågående phishing-attack. Granskningen visade även att medarbetarna använde sig av olika rapporteringsvägar för att rapportera e-postmeddelandet under den simulerade phishing-attacken.

EY anser att man med fördel bör begränsa antalet rapporteringskanaler för att få en effektiv och samlad rapportering. Detta eftersom det vid en pågående säkerhetsincident likt phishing är avgörande att kommunens incidenthanteringspersonal snabbt kan bilda sig en förståelse av vad som har inträffat. EY rekommenderar således kommunstyrelsen att rapporteringsvägarna begränsas och kommuniceras till samtliga medarbetare inom kommunen.

Utöver detta rekommenderar EY att man inom Södertälje kommun arbetar vidare med att kommunicera vikten av att rapportera eventuella säkerhetsincidenter. Kommunikationen bör inkludera tydliga förväntningar och kravställningar på rapportering hos samtliga medarbetare då man misstänker att man blivit utsatt för en phishing-attack. Detta för att öka sannolikheten att fler medarbetare väljer att rapportera en säkerhetsincident relaterat till phishing.

3.3 Teoretiska och praktiska utbildningar inom phishing

I takt med att mängden cyberattacker mot organisationer har ökat de senaste åren har EY noterat en markant ökning i antalet phishing-attacker. Detta kan bland annat ha berott på covid-19 och den ökade användningen av digitala verktyg. Medarbetares medvetenhet och kunskap om informationssäkerhet blir således allt viktigare för att säkerhetsställa ett adekvat skydd av informationen hos en organisation. Vidare ställs krav på att uppfylla lagar och regleringar om informationssäkerhet och dataskydd. En phishing-attack kan leda till allvarliga konsekvenser för kommunen, dels genom att utvinna känslig och konfidentiell information, dels genom att implementera skadlig kod på mottagarens enhet.

Den simulerade övningen visade att 28,8 procent av samtliga mottagare klickade på länken i e-postmeddelandet och att 7,7 procent av samtliga mottagare uppgav sin användardata på landningssidan. Baserat på resultatet och de satta acceptansnivåerna löper Södertälje kommun en mycket hög risk för att utsättas för en fullbordad phishing-attack. Med anledning av detta rekommenderar EY att utbildningar inom informationssäkerhet och phishing planeras och följs upp för alla medarbetare inom kommunen. Därtill rekommenderar EY att man inom kommunen undersöker kunskapsbehoven hos medarbetare och därefter inför anpassade utbildningsinsatser.

Specifik utbildning inom phishing syftar till att förbättra medvetenheten och kunskapen om just denna typ av attack genom hela kommunen. Resultatet från granskningen visar även på vilka delar av kommunen som löper störst risk och där riktade utbildningsinsatser kan behövas. Det kan vara kontor i särskilt hög riskgrupp, med anledning av verksamhetens syfte och känslighetsgraden av informationen som hanteras. EY rekommenderar att kommunstyrelsen säkerställer att utbildningar som ger medarbetare kunskapen att kunna identifiera falska e-postmeddelanden, domäner och hemsidor erbjuds för samtliga medarbetare. EY rekommenderar vidare att det inom utbildningarna ska finnas utrymme för diskussioner och möjligheter till övning för att jämföra sofistikerade falska e-postmeddelanden med autentiska e-postmeddelanden. Utöver specifika utbildningstillfällen rekommenderar EY att utbildningsmaterial kontinuerligt sprids till medarbetarna, exempelvis i form av checklistor medarbetarna kan följa vid misstanke av en phishing-attack.

EY rekommenderar vidare att kommunstyrelsen säkerställer att utbildningarna följs upp med 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. Det finns olika tillvägagångssätt på vilka en kommun kan testa medvetenheten hos medarbetarna, såsom interaktivt utbildningsmaterial och nätbaserade simulationer. Inför den simulerade övningen noterade EY att servicedesk satte en gräns på att hantera maximalt 20 ärenden över normal belastning under en dag. Då detta begränsar möjligheten att praktiskt öva och testa medarbetarnas förmåga att identifiera phishing-attacker rekommenderar EY att kommunstyrelsen tillser att det sker en översyn kring överenskommelsen med leverantören som sköter servicedesk. Slutligen rekommenderar EY att man inom Södertälje kommun fortsätter med uppföljande simuleringar av phishing-attacker för att praktiskt testa medarbetarnas kunskap och medvetenhet, samt för att samla in enhetliga data.

4. Revisionsfrågor

Granskningen har utgått från tre revisionsfrågor. Hur väl Södertälje kommun svarar upp mot dessa revisionsfrågor beskrivs nedan.

Färgkod	Förklaring
	Revisionsfråga besvaras ej tillfredsställande
	Revisionsfråga besvarad delvis tillfredsställande
	Revisionsfråga besvaras tillfredsställande

Revisionsfråga	Svar
<p>▶ Hanterar Södertälje kommuns medarbetare hotet från attacker genom falska e-postmeddelanden, så kallad phishing, på ett ändamålsenligt sätt?</p>	<p>Baserat på den genomförda granskningen bedömer EY att Södertälje kommun bör arbeta för att förbättra sin motståndskraft mot phishing. Bedömningen baseras på resultatet av simuleringen där 28,8 procent av mottagarna klickade på länken. Resultatet tyder på att kommunen löper en mycket hög risk att utsättas för en fullbordad phishing-attack. Därutöver uppgav 7,7 procent av mottagarna användarinformation. EY vill betona att det räcker med att en användare uppger användarnamn och lösenord för att en angripare ska komma åt kommunens IT-miljöer.</p> <p>Slutsatsen är att Södertälje inte hanterar hotet från phishing-attacker på ett ändamålsenligt sätt. Detta då EY bedömer att motståndskraften mot phishing ligger på en nivå under det man bör förvänta sig av jämförbara organisationer inom den kommunala sektorn.</p>
<p>▶ Har Södertälje kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av de testade medarbetarna under den simulerade attacken?</p>	<p>Södertälje kommuns incidenthanteringsprocess är dokumenterad och finns att hitta på intranätet. Kommunens medarbetare uppmanas att kontakta antingen IT-säkerhetsavdelningen eller servicedesk vid ett misstänkt e-postmeddelande. Då medarbetarna hänvisas till olika e-postadresser kan otydliga instruktioner leda till att få följer incidenthanteringsprocessen.</p> <p>Därutöver visade simuleringen att medarbetare valt att rapportera till enstaka personer inom IT-enheten och IT-säkerhetsavdelningen. Det här tyder på att det finns olika sätt att rapportera</p>

	<p>incidenter på och att rapporteringen är personbaserad, vilket kan leda till ineffektiv hantering av incidenter.</p> <p>Därmed bedömer EY att kommunen inte har en incidenthanteringsprocess som aktiverats på ett ändamålsenligt sätt av medarbetarna under den simulerade attacken.</p>	
<p>► Är riktlinjer för hantering och rapportering av falska e-postmeddelanden och andra incidenter kända hos medarbetarna?</p>	<p>I Södertälje kommun finns dokumenterade riktlinjer för hur medarbetare ska hantera ett förmodat falskt e-postmeddelande vid en phishing-attack.</p> <p>Granskningen visar att medarbetarna i stor utsträckning uppger att riktlinjerna är svåra att förstå och att många medarbetare inte känner till dem. Därutöver visar enkätresultatet att medarbetarna inte vet hur och till vem de ska rapportera en pågående phishing-attack. Detta försvårar för kommunen att ha en god beredskap vid en pågående phishing-attack</p> <p>Således bedömer EY att kommunen delvis har kommunicerat instruktioner och riktlinjer för informationssäkerhet till medarbetarna på ett tillfredsställande sätt.</p>	

5. Slutsatser

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

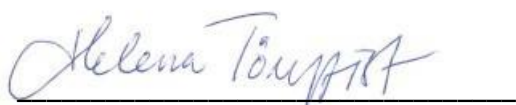
- ▶ Hanterar Södertälje kommuns medarbetare hotet från attacker genom falska e-postmeddelanden, så kallad phishing (nätfiske), på ett ändamålsenligt sätt?
- ▶ Har Södertälje kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av de testade medarbetarna under den simulerade attacken?
- ▶ Är riktlinjerna för hantering och rapportering av falska e-postmeddelanden och andra incidenter kända hos medarbetarna?

Resultatet visar att det finns ett behov av att förbättra utbildning och medvetenhet inom IT- och informationssäkerhet och phishing, då en stor andel medarbetare inte har tillräcklig kunskap inom området för att kunna identifiera ett falskt e-postmeddelande. Vidare visade resultatet av enkäten på att en stor andel av medarbetarna inte är medvetna om kommunens riktlinjer för informationssäkerhet, eller hur de ska gå till väga för att rapportera en säkerhetsincident relaterad till e-postmeddelanden. Kommunstyrelsen rekommenderas därför att vidta åtgärder för att informera om relaterade styrdokument och riktlinjer, begränsa antalet rapporteringsvägar för att få en effektiv och samlad rapportering, och stärka utbildning och medvetenheten hos medarbetarna. En förbättrad motståndskraft mot phishing kan bidra till att förluster av känslig information, negativt rykte eller andra betydande konsekvenser minimeras.

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

- ▶ Informera om riktlinjer för informationssäkerhet och phishing.
- ▶ Tydliggör och informera om rutiner för rapportering av misstänkta e-postmeddelanden.
- ▶ Inför både teoretiska och praktiska utbildningar inom informationssäkerhet och phishing.

Stockholm, 2022-12-05



Helena Törnqvist

Partner, EY

Bilaga 1: E-postmeddelande

E-postmeddelande

Från: Ekonomi <faktura-ekonomi@sodertaljekomun.se>

Datum: 5 oktober 2022 10:51:33 CEST

Till:

Ämne: Viktigt: status på faktura

Hej,

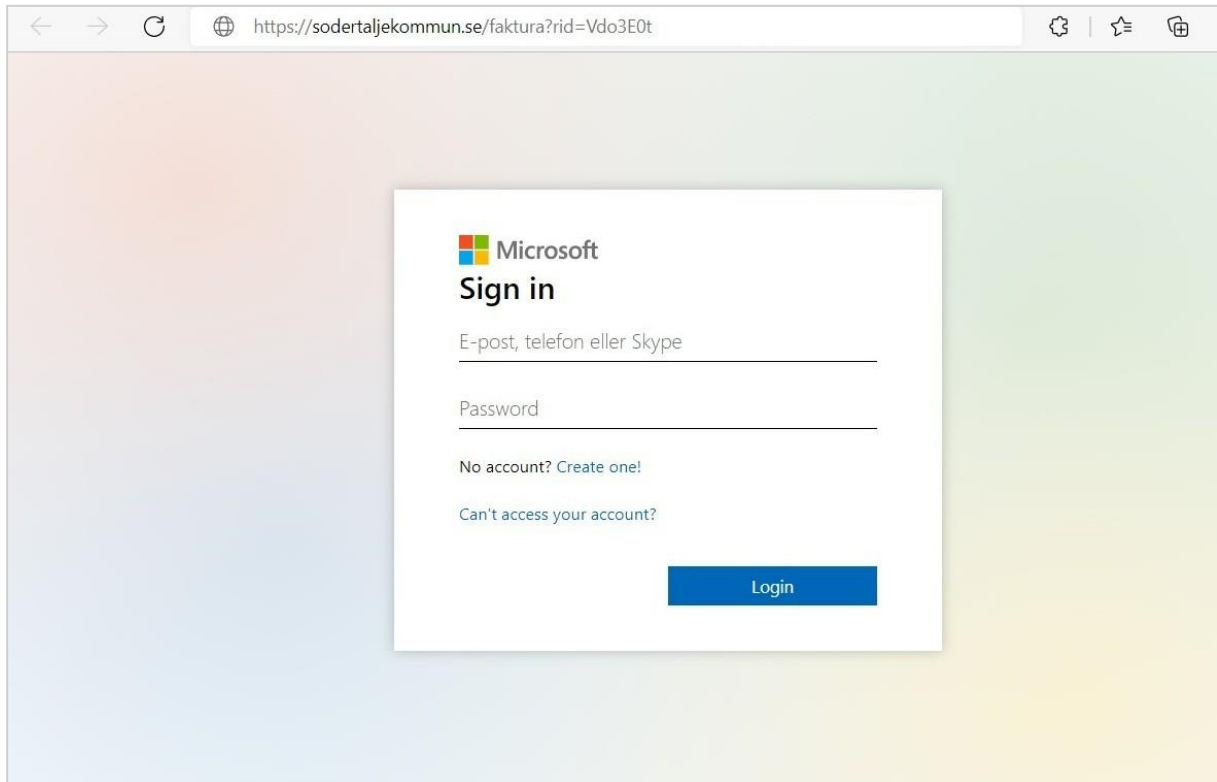
Vi har noterat att du har öppnade faktura i systemets fakturasystem.

Du har fakturor som är nära att förfalla till betalning eller har redan förfallit. Det är viktigt att du betalar fakturorna så fort som möjligt, helst redan nu. Detta tar bara några minuter av din tid. [Klicka här](#) för att se över dina fakturor.

Med vänliga hälsningar,
Ekonomiavdelningen

Bilaga 2: Landningssida

Landningssida 1



The screenshot shows a web browser window with the address bar containing the URL <https://sodertaljekommun.se/faktura?rid=Vdo3E0t>. The page content is a Microsoft Sign in dialog box. At the top left of the dialog is the Microsoft logo. Below it, the text "Microsoft" is displayed in a grey font, followed by "Sign in" in a larger, bold black font. There are two input fields: the first is labeled "E-post, telefon eller Skype" and the second is labeled "Password". Below the input fields, there are two links: "No account? Create one!" and "Can't access your account?". At the bottom right of the dialog is a blue button labeled "Login".

Landningssida 2

OBS! Detta e-postmeddelande var nätfiske.

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

Denna övning utfördes i samarbete med EY som en del av kommunens arbete inom informationssäkerhet. Vi hoppas med den här övningen 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 mejl med kollegor eller informerar dem om övningen.



Stanna upp, se efter, tänk till!

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 @sodertaljekomun.se från vilken e-postmeddelandet skickades är inte en domän som Södertälje kommun använder utan en så kallad bluffdomän. Dessa är gjorda så att man vid första anblick inte ska misstänka att någonting är fel.

Om du misstänker att du har utsatts för en phishing-attack, kontakta genast servicedesk hos kommunen.

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 @sodertaljekomun.se från vilken e-postmeddelandet skickades är inte en domän som Södertälje 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 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.

3. Kontrollera språket

Håll utkik efter stavfel. Seriosa 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.

Mer information om nätfiske hittar du här: <https://kanalen.sodertalje.se/stod-i-arbetet/saker-informationshantering/natfiske-e-post-och-bluffmejl/>

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, och 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 phishing-attack är och hur man ska reagera på sådana attacker

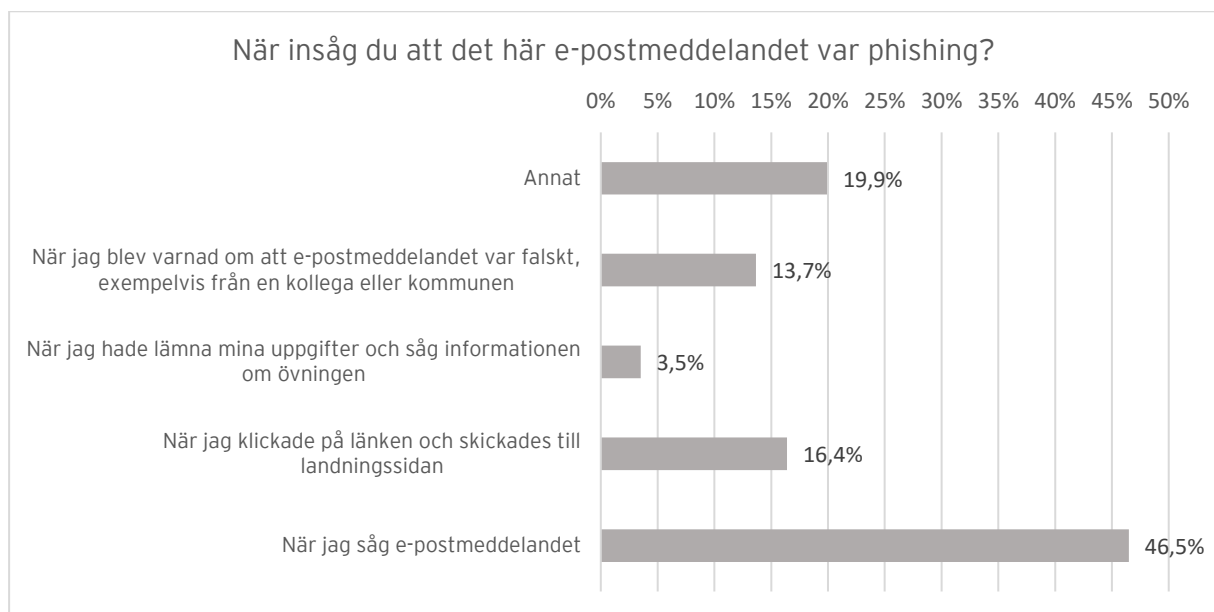
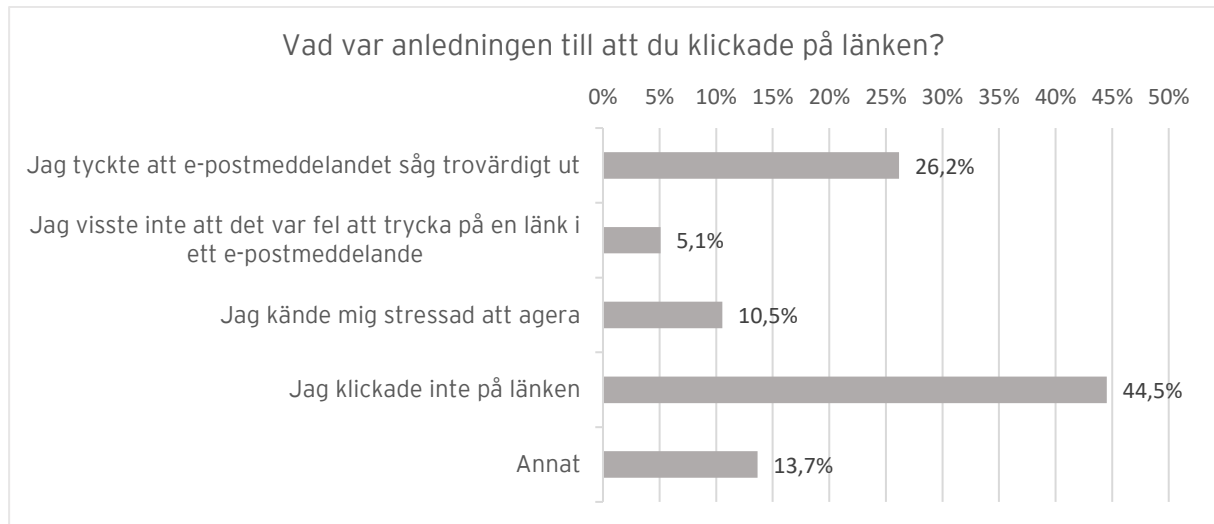
Policy och riktlinjer

- Jag känner till kommunens informationssäkerhetspolicy samt relaterade riktlinjer
- Jag tycker att informationssäkerhetspolicyen 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.

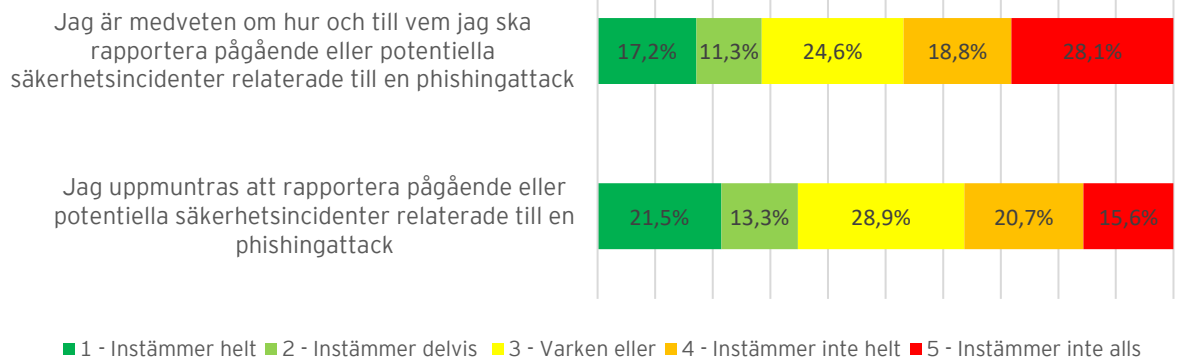
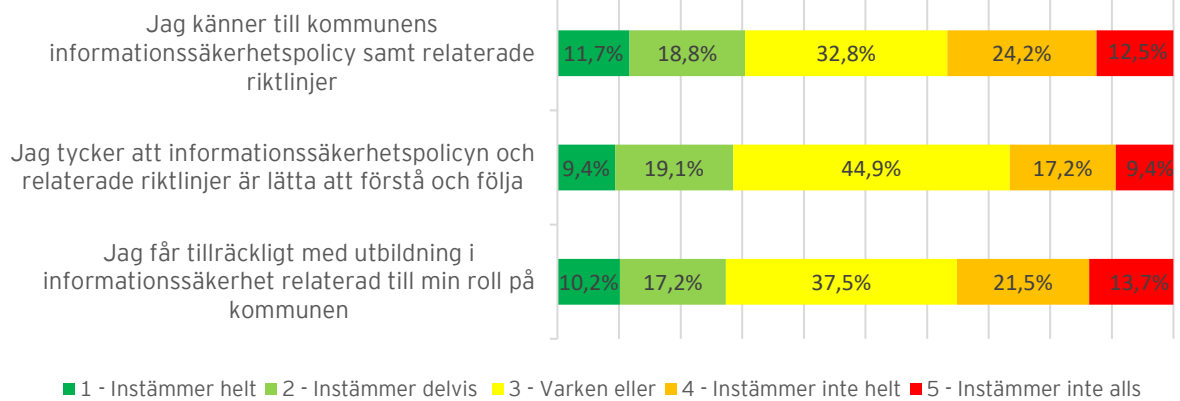
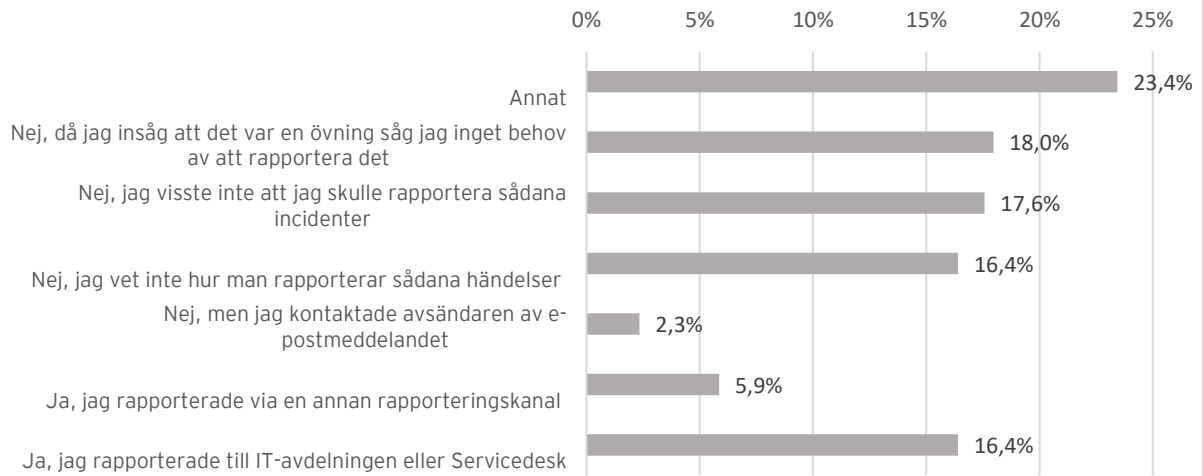
Rapportering

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

Bilaga 5: Enkätresultat



Rapporterade du e-postmeddelandet?



Bilaga 6: Definitioner

Acceptansnivåer: Acceptansnivåer är ett sätt att översätta generella och övergripande risknivåer till aktuella måttetal 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 phishing-attacker 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 och organisationer. Metoden går ut på att utforma på olika sätt men går generellt 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 phishing-attacker 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.