Tyresö kommun

Rapport: Informationssäkerhet i praktiken
September 2023

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Tyresö kommun har EY genomfört en granskning med syfte att bedöma om det finns brister i det praktiska arbetet inom IT-och informationssäkerhet, exempelvis genom att testa medarbetarnas medvetenhet och kunskap inom området. Detta bedöms bland annat genom att simulera ett angrepp via e-post, där kommunens tekniska skydd har kopplats bort.

Följande revisionsfrågor har legat till grund för granskningen:

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

Granskningen genomfördes från maj till augusti 2023. EY utformade och genomförde granskningen tillsammans med representanter från kommunen i syfte att uppnå en så stor nytta som möjligt för verksamheten. 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 inom offentlig sektor.

Baserat på genomförd granskning bedömer EY att det finns brister gällande utbildning och medarbetarnas medvetenhet inom informationssäkerhet i Tyresö kommun. Kommunen som helhet löper en *medelhög risk* att utsättas för en fullbordad phishing-attack, men EY noterar att för en majoritet av kommunens förvaltningar är risken att betrakta som *hög* eller *mycket hög*. Det räcker med att endast en anställd lämnar ut sina användaruppgifter för att angriparen ska kunna ta sig in i kommunens IT-miljö och därför anser EY att det är denna högre risk som kommunen har att hantera.

Kommunstyrelsen rekommenderas därför att vidta åtgärder för att förbättra sin motståndskraft mot phishing och således minska risken från phishing-attacker. 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.
- Genomför teoretiska och praktiska utbildningar inom phishing.

Innehållsförteckning

1. Bakgrund

Tyresö kommun, inklusive dess nämnder och förvaltningar, 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 informationssäkerhet 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 informationssäkerhet. Revisorerna har därför valt att genomföra en granskning för att testa hur väl kommunens riktlinjer och rutiner med IT- och informationssäkerhet 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 informationssäkerhetsarbete 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 i enlighet med vad som uppmanas av kommunen 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 informationssäkerhetsrisker. 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. Denna typ av manipulation kan ske på olika sätt, exempelvis genom att övertyga medarbetaren att besöka skadliga hemsidor och ladda ner skadlig programvara. Manipulation kan även ske genom att den cyberkriminella får medarbetaren att uppge viktig information genom telefon, så kallad *vishing*, eller att ansluta ett USB-minne till organisationens nätverk. Det finns även andra mänskliga faktorer vilka medför risker, som användning av svaga lösenord, eller att samma lösenord används på flera, viktiga platser.

Under covid-19-pandemin har EY sett en ökning av den typ av cyberkriminalitet som bygger på social manipulation, 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 informationssäkerhet 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 för

organisationen att arbeta proaktivt för att hantera det ökade hotet från phishing. Ett viktigt tillvägagångssätt för detta är att skapa och bibehålla en medvetenhet om hotet från phishing hos medarbetare inom en organisation 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 informationssäkerhet. 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 i Tyresö kommun 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. Följande revisionsfrågor har legat till grund för granskningen:

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

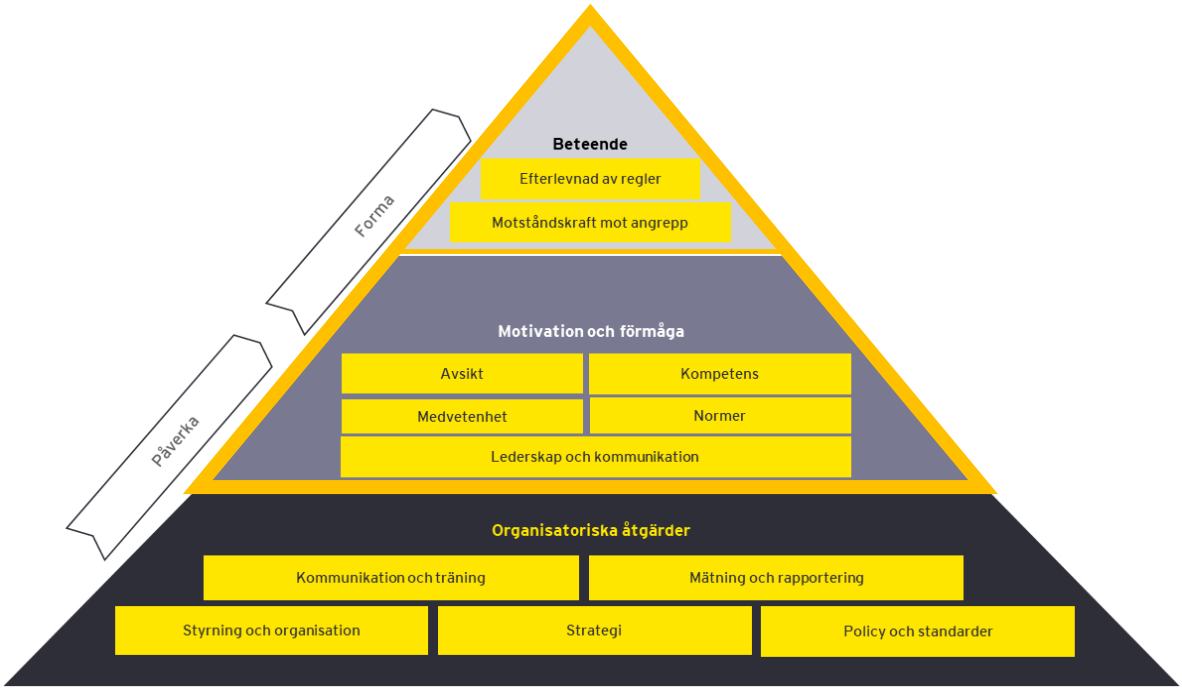
1.3 Avgränsningar

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 att 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 Tyresö 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 medarbetarne 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 Tyresö 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 informationssäkerhet.

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 Tyresö 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 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 utvinner känslig information och tar 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 som valde 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 deras kunskap om hur de ska 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 Tyresö 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. Det 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 Servicedesk, men skickades från en e-postadress med domänen "tyreso.info", vilket är en domän som inte tillhör Tyresö kommun. I e-postmeddelandet fick mottagaren veta att deras inkorg är full, och att mottagaren inte kommer kunna skicka eller ta emot nya e-postmeddelanden innan inkorgens utrymme har ökat. Mottagaren blev därefter uppmanad att klicka på en länk för att öka utrymmet i sin inkorg. Genom att följa länken i e-postmeddelandet landade besökaren på den förfalskade landningssidan där de ombads logga in med ett 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 risk att bli utsatt för en fullbordad phishing-attack (risknivåer). Se avsnitt *1.4.2.5 Risknivåer och acceptansnivåer* för vidare förklaring av hur risknivåer kan definieras vid en phishing-attack. 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 alla kommunens medarbetare skulle delta i simuleringen. Detta resulterade i att 3775 medarbetare deltog i övningen.

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[1]. Detta innebär att delar av kommunens tekniska skydd mot phishing kopplas bort, i syfte att på ett kostnadseffektivt sätt testa personalen och inte tekniken. Dessutom togs en varningstext bort som vanligtvis finns på externa mail, vilket ökar svårigheten för medarbetarna att avgöra huruvida e-postmeddelandet är falskt eller inte. Det bör noteras att inget tekniskt skydd fullständigt kan förhindra ett angrepp via phishing. EY genomförde simuleringen under vecka 22.

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 rapporteringsvägar existerar och att medarbetarna är medvetna om hur dessa ska

[1] För förklaring av begreppen, se definitioner i *bilaga 6*.

användas. 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. Åtgärder mot phishing-attacken bör vidtas skyndsamt då hotet är som störst under den initiala tiden efter att e-postmeddelandet mottagits.

På Tyresö kommuns intranät finns en informationssäkerhetsinstruktion. I denna instruktion tillhandahålls information om vad som typiskt kännetecknar ett falskt meddelande, vilket kan hjälpa medarbetaren kontrollera om ett meddelande är falskt. De signalement som anges i instruktionen inkluderar att meddelandet innehåller en okänd avsändare, tvivelaktig rubrik eller tom ämnesrad, bifogade filer med osäkert innehåll eller syfte, samt bifogade länkar med osäkert innehåll eller syfte. Vid misstanke om felaktiga länkar, skadlig kod i e-postmeddelandet eller en okänd avsändare i ett e-postmeddelande med bifogad fil, uppmanas medarbetaren att rapportera detta till kommunens Servicedesk. Instruktionen informerar även om att kontakt med Servicedesk, vid felanmälan eller support, ska ske via en IT-portal på intranätet. Denna IT-portal är ett ärendehanteringssystem som möjliggör för användaren att både registrera och följa pågående ärenden. IT-portalen är kommunens föredragna rapporteringsväg och kommunen arbetar för att få fler att använda den, bland annat genom att hänvisa till denna i informationssäkerhetsinstruktionen. Servicedesk kan även nås via e-post, telefon och fysiskt besök, och kontaktuppgifter till Servicedesk kommuniceras på intranätet.

Intervjuade nyckelpersoner har även uppgett att det på intranätet publiceras nyheter med uppmaningar om att medarbetarna ska vara vaksamma och att de ska rapportera om de misstänker att de fått ett falskt e-postmeddelande.

1.4.2.4 Enkät

Efter avslutad simulering distribuerades en enkät 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 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 som 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 nödvändiga åtgärder för att minimera 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 mätetal anpassade för den aktuella organisationen, vilka 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 maj 2023 till augusti 2023, se *tabell 2* nedan för granskningens tidsplan.

Tabell 2: Tidsplan

Förberedelser och planering	Maj 2023
Test och utskick	Juni 2023
Rapportskrivning och intern kvalitetssäkring	Juni 2023
Justering och färdigställande av rapport	Augusti 2023
Avrapportering och slutpresentation	September 2023

2. Analys

I följande kapitel analyseras resultatet av den simulerade attack som EY utformat tillsammans med Tyresö kommun. 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-postmeddelandets

I detta avsnitt presenteras andelen mottagare som klickade på länken i e-postmeddelandet. Tyresö 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.

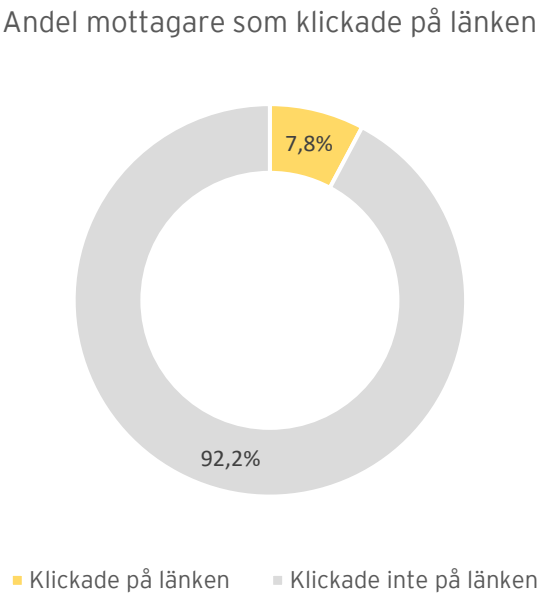
Resultatet av den simulerade attacken visar att 7,8 procent av mottagarna klickade på den inbäddade länken i e-postmeddelandet och att Tyresö kommun som helhet löper en medelhög risk att utsättas för en fullbordad phishing-attack enligt de definierade acceptansnivåerna. EY noterar att ett flertal av förvaltningarna dock löper en *hög eller mycket hög risk* att utsättas för en fullbordad phishing-attack.

Tabell 3: Acceptansnivåer för andelen mottagare som klickar på länken i e-postmeddelandet

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

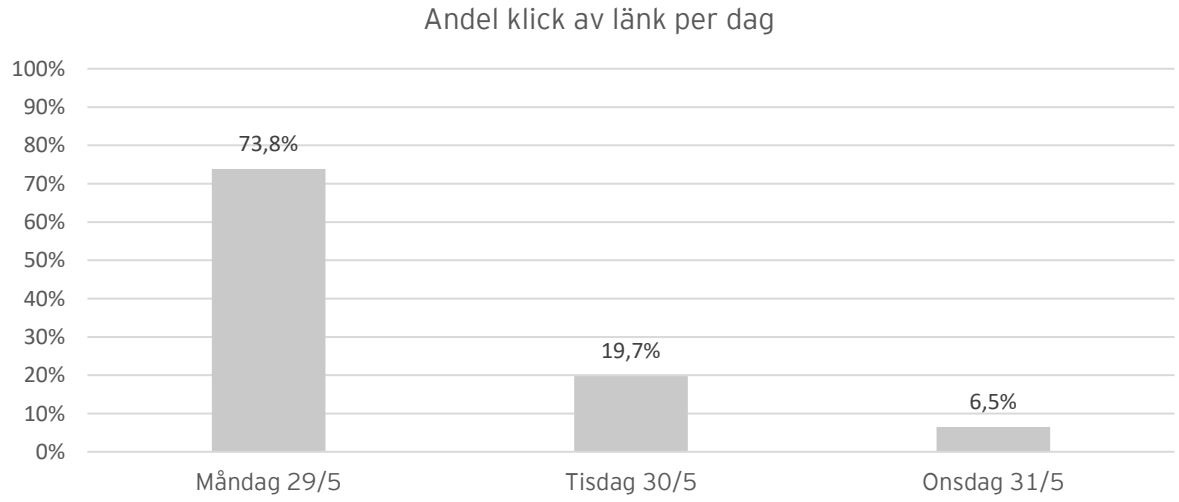
2.1.1 Resultat av simulering

Det insamlade resultatet analyserades utifrån hur många mottagare som klickat på länken i det förfalskade meddelandet, både för kommunen som helhet och uppdelat på kommunens olika förvaltningar. Av 3775 mottagare klickade 294 på länken i e-postmeddelandet, vilket motsvarar ungefär 7,8 procent av mottagarna, se *figur 2* nedan. Det här resultatet innebär enligt acceptansnivåerna att Tyresö kommun som helhet löper en medelhög risk att utsättas för en fullbordad phishing-attack.



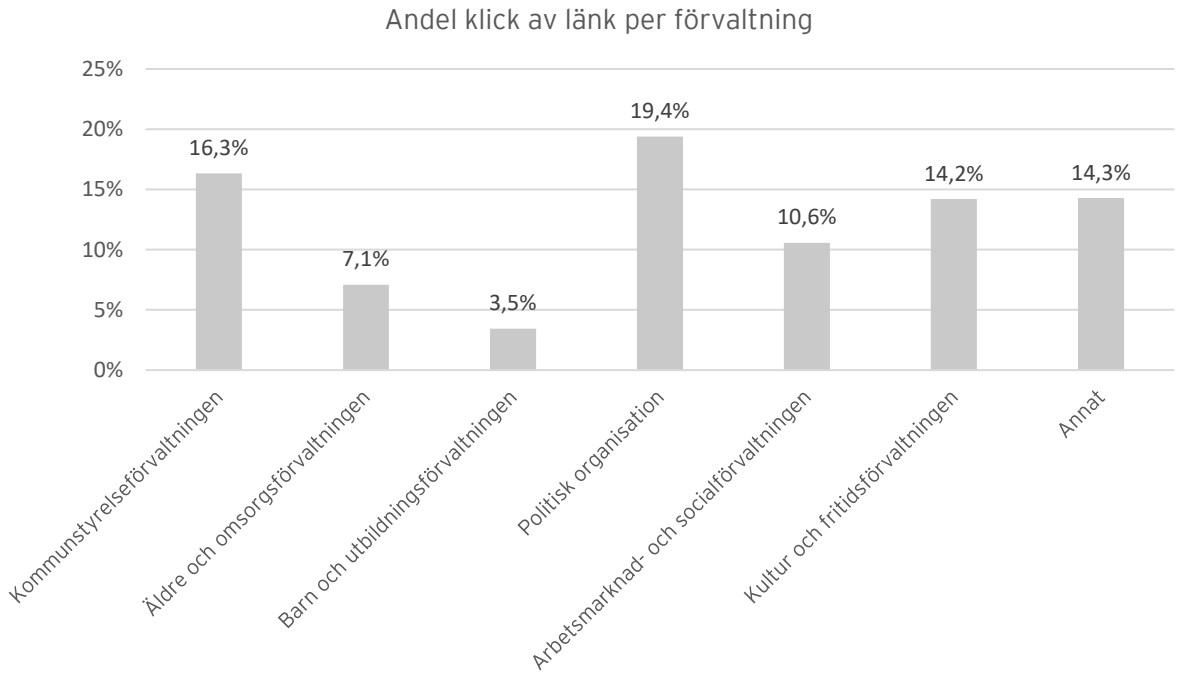
Figur 2: Fördelningen av andel mottagare som klickade på länken i e-postmeddelandet. Resultatet beskriver kommunen som helhet, dvs. inkluderat kommunens olika förvaltningar.

Simuleringen var aktiv under vecka 22 och resultatet samlades in mellan måndag 29/5 och onsdag 31/5. Samtliga e-postmeddelanden skickades ut under morgonen, måndag 29/5. I *Figur 3* illustreras andelen klick på den inbäddade länken per dag. Från figuren framgår det att en stor majoritet (73,8 procent) av mottagarna som klickade på länken i e-postmeddelandet gjorde detta under simuleringens första dag. Vidare utfördes 19,7 procent av klicken under den andra dagen, och endast 6,5 procent under den tredje dagen. EY noterar därmed att antalet klick på länken sjönk markant under de två nästkommande dagarna efter simuleringens start. Den här trenden är enligt EY förväntad i simulerade phishing-attacker likt den som genomförts i Tyresö kommun, som påkallar omedelbara handlingar från mottagaren utifrån hur e-postmeddelandet är formulerat.



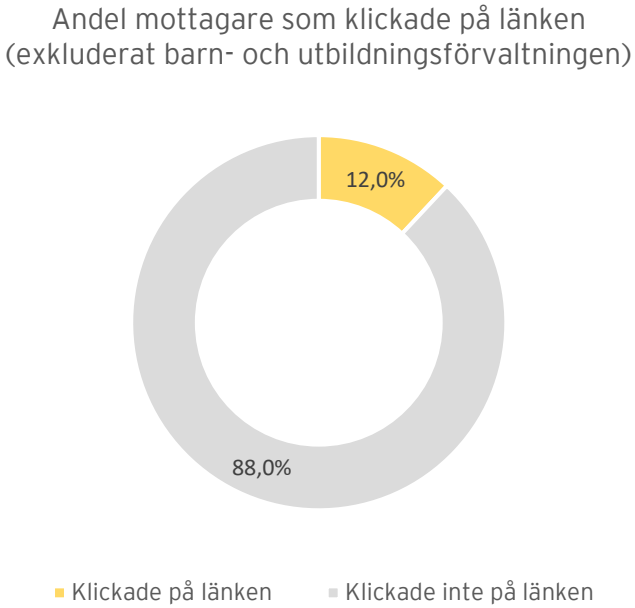
Figur 3: Andelen klick på den inbäddade länken per dag, under simuleringens aktiva period. Resultatet beskriver kommunen som helhet, dvs. inkluderat kommunens olika förvaltningar.

Figur 4 visar andelen klick på länken i e-postmeddelandet per förvaltning. EY noterar att andelen klick per förvaltning varierar mellan låg risk och mycket hög risk i jämförelse med de på förhand bestämda acceptansnivåerna. EY noterar vidare att den politiska organisationen hade den högsta andelen mottagare som klickade på länken med 19,4 procent. Tillsammans med kommunstyrelseförvaltningen på 16,3 procent medarbetare som klickade på länken ligger denna förvaltning på en mycket hög risk att utsättas för en fullbordad phishing-attack i jämförelse med acceptansnivåerna. Vidare noterar EY att arbetsmarknads- och socialförvaltningen, kultur och fritidsförvaltningen samt "Annat" ligger på andelar som indikerar en hög risk. Lägst andel mottagare som klickade på länken hade barn och utbildningsförvaltningen, som ligger på en låg risk enligt acceptansnivåerna.



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. "Annat" syftar på personer som inte hade någon tilldelad förvaltning, samt förvaltningar med ett fåtal medarbetare.

EY noterar även att barn och utbildningsförvaltningen är den förvaltning med flest antal medarbetare (1854) vilket motsvarar 49,1 procent av simuleringens mottagare. Eftersom denna förvaltning utgör en så stor del av kommunens medarbetare i kombination med att dess andel klick indikerar en låg risk, resulterar det i att förvaltningen drar ner kommunens genomsnittliga resultat av andel klick som illustreras i *figur 2*. EY noterar även att simuleringen genomfördes under en tid då medarbetare inom barn och utbildningsförvaltningen naturligt var mindre aktiva med arbete som berör e-post. I *figur 5* framgår det att andelen mottagare som klickat på länken när barn och utbildningsförvaltningen exkluderats uppgår till 12 procent vilket enligt acceptansnivåerna indikerar en hög risk för att utsättas för en fullbordad phishing-attack. Detta kan jämföras med *figur 2*, där andelen var 7,8 procent då barn och utbildningsförvaltningen inkluderas.



Figur 5: Fördelningen av andel mottagare som klickade på länken i e-postmeddelandet. Notera att i denna figur har barn-och utbildningsförvaltningen exkluderats.

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 första landningssidan. Tyresö kommun hade i samråd med EY på förhand bestämt acceptansnivåer baserat på verksamhetens omfattning. *Tabell 4* beskriver beslutade acceptansnivåer för andelen mottagare som uppger användarinformation.

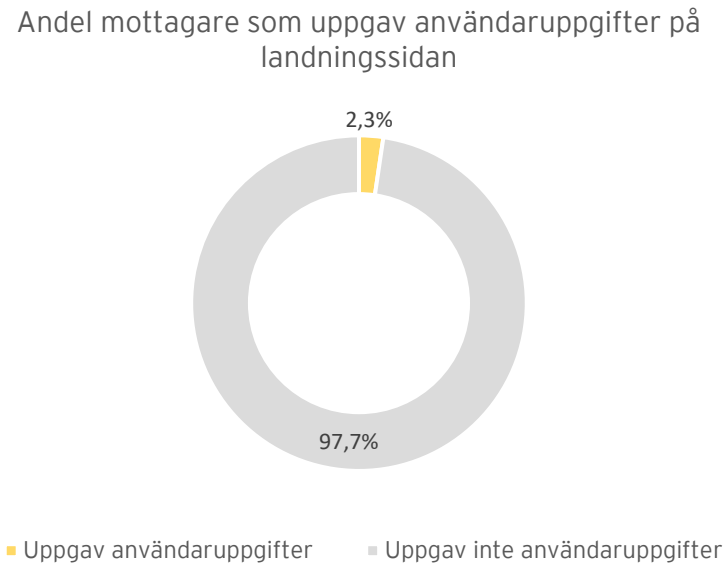
Resultatet av den simulerade attacken för kommunen som helhet visar att 2,3 procent av alla mottagare uppgav sin användarinformation på den förfalskade landningssidan. I relation till de på förhand definierade acceptansnivåerna indikerar resultatet att Tyresö kommun löper en medelhög risk att utsättas 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 uppger användarinformation på landningssidan

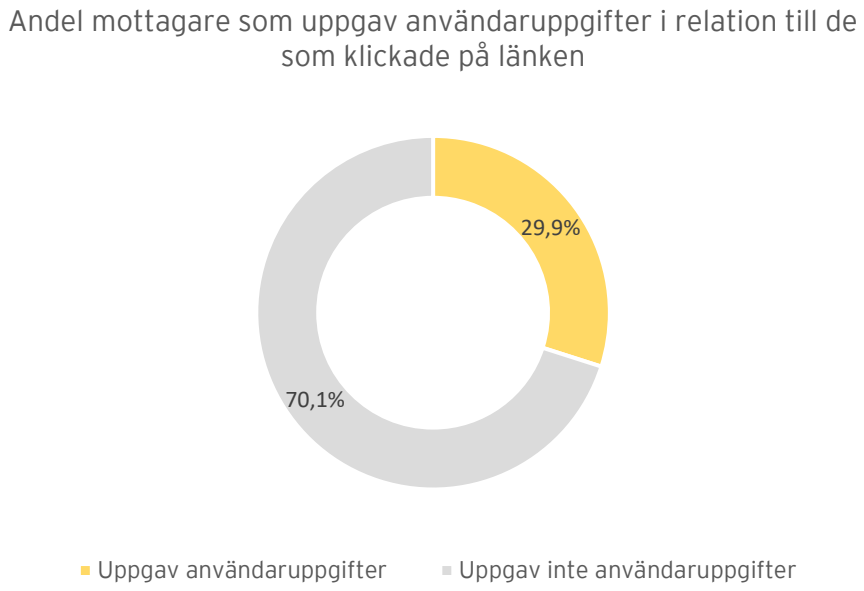
Riskanalys	Acceptansnivå (%)
Mycket hög risk	>6%
Hög risk	4-6%
Medelhög risk	2-4%
Låg risk	<2%

2.2.1 Resultat av simulering

Av det totala antalet mottagare (3775), klickade 88 medarbetare på länken samt uppgav sin användarinformation i form av användarnamn och lösenord på landningssidan. Det motsvarar 2,3 procent av alla mottagare, se *figur 6*. I jämförelse med acceptansnivåerna i *tabell 4*, löper därmed Tyresö kommun som helhet en medelhög risk att utsättas för en fullbordad phishing-attack. Från *figur 7* kan det även noteras att 88 av de 294 medarbetare, det vill säga 29,9 procent, som klickade på länken även uppgav användarinformation, medan resterande valde att lämna landningssidan.

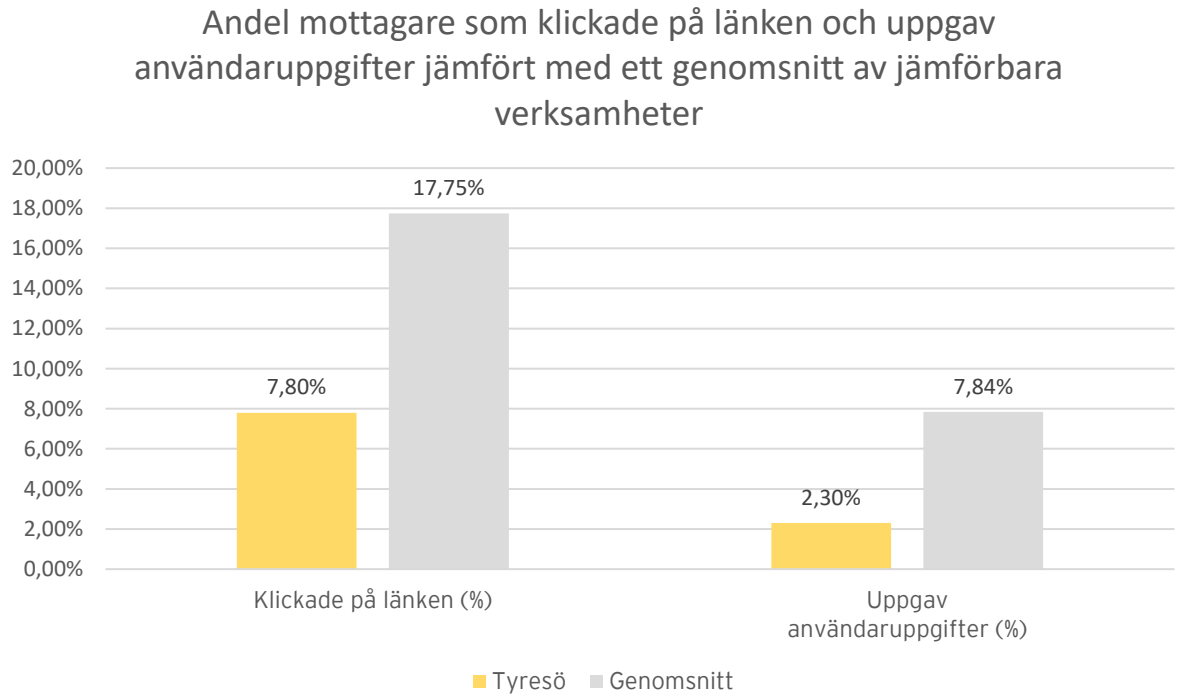


Figur 6: Fördelningen av andel mottagare som uppgav användaruppgifter på landningssidan. Resultatet beskriver kommunen som helhet, dvs. inkluderat kommunens olika förvaltningar.



Figur 7: Fördelningen av andel mottagare som uppgav användaruppgifter på landningssidan i relation till de mottagare som enbart klickade på länken. Resultatet beskriver kommunen som helhet, dvs. inkluderat kommunens olika förvaltningar.

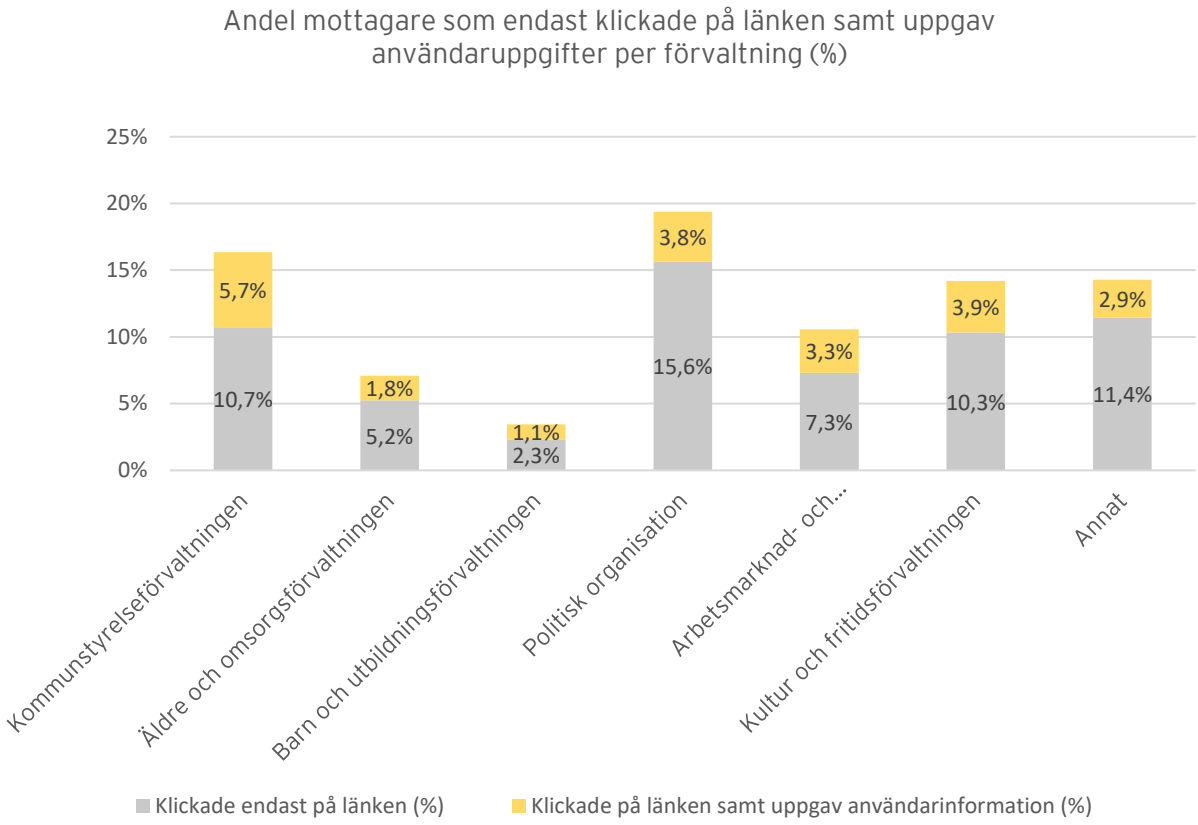
I *figur 8* visas andelen mottagare som klickade på den inbäddade länken samt andelen som uppgav användaruppgifter för Tyresö kommun i jämförelse med ett genomsnitt framtaget för jämförbara verksamheter. Från denna figur ligger Tyresö kommun 9,95 procentenheter under genomsnittet med avseende på andelen mottagare som klickade på länken, samt 5,54 procentenheter under genomsnittet för andelen som uppgav användaruppgifter.



Figur 8: Andel mottagare som klickade på den inbäddade länken samt andel mottagare som uppgav användaruppgifter på landningssidan. I figuren jämförs Tyresö kommun med ett genomsnitt som baseras på jämförbara verksamheter.

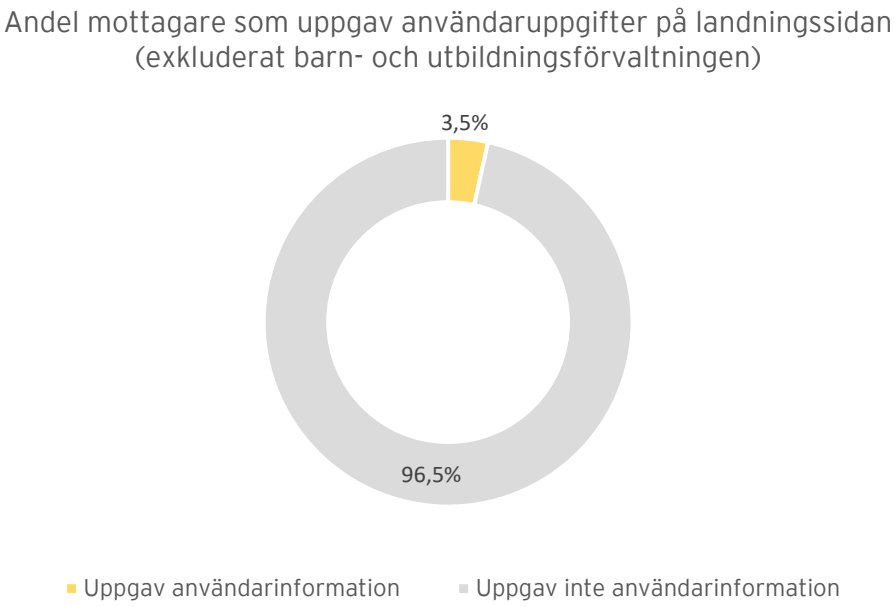
Figur 9 visar andelen mottagare i kommunens olika förvaltningar som klickade på länken i e-postmeddelandet i relation till andelen mottagare som utöver att klicka på länken även uppgav användarinformation på landningssidan. Resultaten visar att kommunstyrelseförvaltningen var den förvaltning med högst andel medarbetare som uppgav användarinformation, nämligen 5,7 procent. Denna förvaltning löper enligt acceptansnivåerna en hög risk för att utsättas för en fullbordad phishing-attack. Resultaten visar även på en medelhög risk för förvaltningar såsom kultur och fritidsförvaltningen, den politiska organisationen samt arbetsmarknads- och socialförvaltningen med 3,9 procent, 3,8 procent respektive 3,3 procent. I barn- och utbildningsförvaltningen var det endast 1,1 procent som uppgav användarinformation och i äldre- och omsorgsförvaltningen endast 1,8 procent, vilket för båda förvaltningarna motsvarar låg risk.

Baserat på acceptansnivåerna noterar EY därmed att förvaltningarnas risk varierar. Riskerna att utsättas för en fullbordad phishing-attack bedöms ligga mellan låg och hög beroende på förvaltning. EY vill betona att det vid en verklig attack kan räcka med att endast en användare uppger sin användarinformation för att den cyberkriminella aktören ska kunna utföra ett lyckat intrång och, i värsta fall, ta kontroll över kommunens IT-miljöer.



Figur 9 : Andelen mottagare som endast 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.

På samma sätt som tidigare tas statistik fram som visar hur andelen mottagare som uppgav användarinformation skiljer sig när barn- och utbildningsförvaltningen exkluderats från resultatet. Denna statistik återfinns i *figur 10*. Anledningen att EY väljer att analysera resultatet på detta sätt är för att förvaltningen omfattar 49,1 procent av alla medarbetare som mottog e-postmeddelandet och att simuleringen gjordes under en period då medarbetarna i denna förvaltning generellt upplever en lägre aktivitet kring sin e-post (vilket antas innebära en lägre risk). Exkluderat barn och utbildningsförvaltningen ökar andelen lämnade användaruppgifter till 3,5 procent vilket visar på en högre risk hos flera av förvaltningarna.



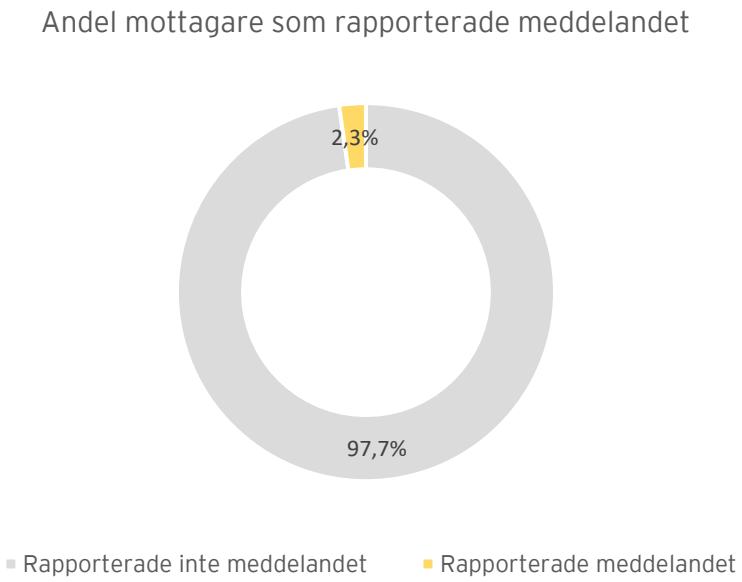
Figur 10: Fördelningen av andel mottagare som uppgav användaruppgifter på landningssidan i relation till de mottagare som enbart klickade på länken. Notera att i denna figur har barn- och utbildningsförvaltningen exkluderats.

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 de anställda i Tyresö 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, policy och rutiner, samt rapportering av säkerhetsincidenter. Enkäten skickades ut till samtliga 3775 deltagare, varav 667 deltog i enkätundersökningen. Notera att i denna analys presenteras ett urval av enkätresultaten (se *bilaga 4* för den fullständiga enkäten och *bilaga 5* för samtliga enkätresultat).

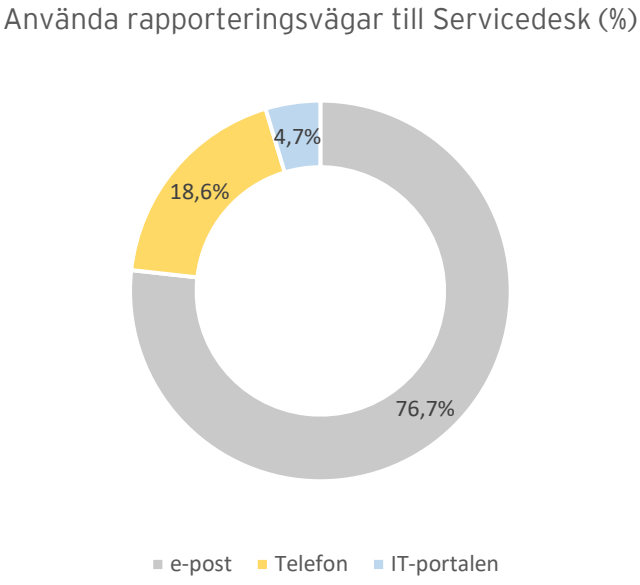
2.3.1 Rapportering

Enligt Tyresö kommuns informationssäkerhetsinstruktionen som EY tagit del av ska misstänksamma e-postmeddelanden rapporteras till kommunens Servicedesk. Detta ska helst ske genom en IT-portal som kan nås av medarbetaren via kommunens intranät. *Figur 11* visar att 86 av 3775 medarbetare rapporterade e-postmeddelandet under pågående simulering, vilket motsvarar 2,3 procent av alla mottagare.



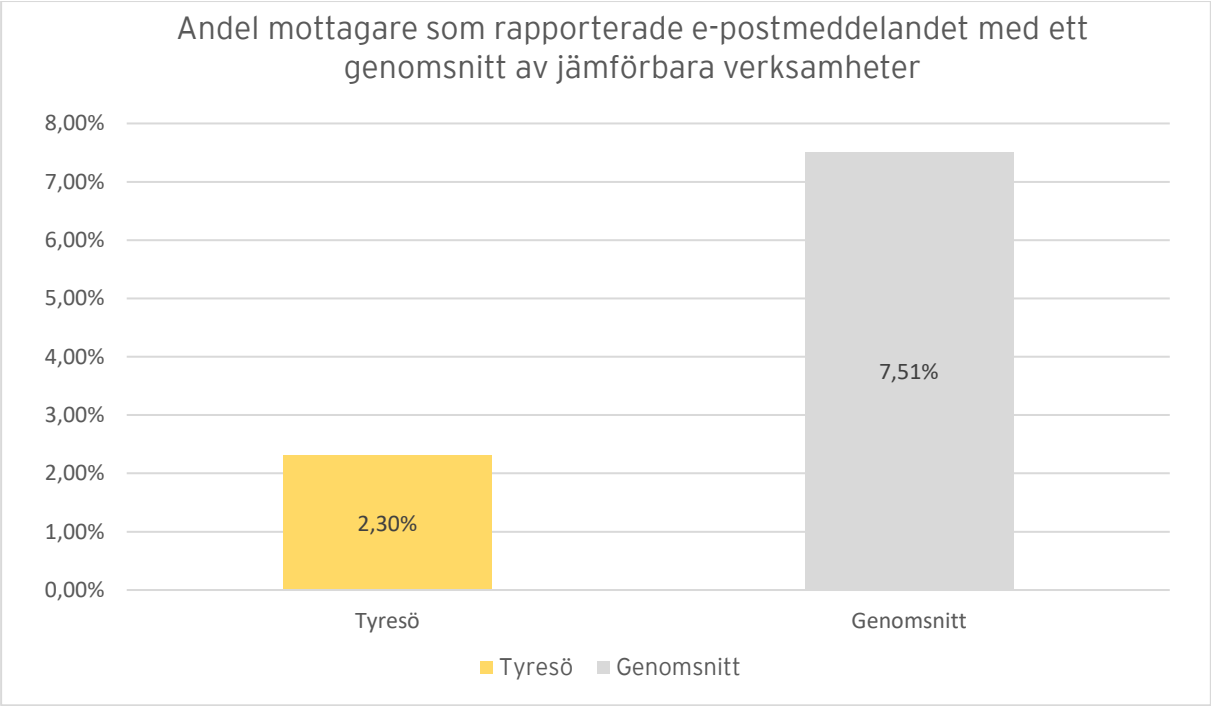
Figur 11: Fördelningen av andel mottagare som rapporterade meddelandet. I detta resultat inkluderas alla möjliga rapporteringsvägar.

Alla uppmätta rapporteringar skedde till Servicedesk, men genom olika rapporteringsvägar. *Figur 12* visar att 76,7 procent av medarbetare som rapporterade e-postmeddelandet gjorde detta till Servicedesk via e-post. Vidare kontaktade 18,6 procent av medarbetarna Servicedesk via telefon och endast 4,7 procent via IT-portalen.



Figur 12: Fördelning av använda rapporteringsvägar under pågående simulering.

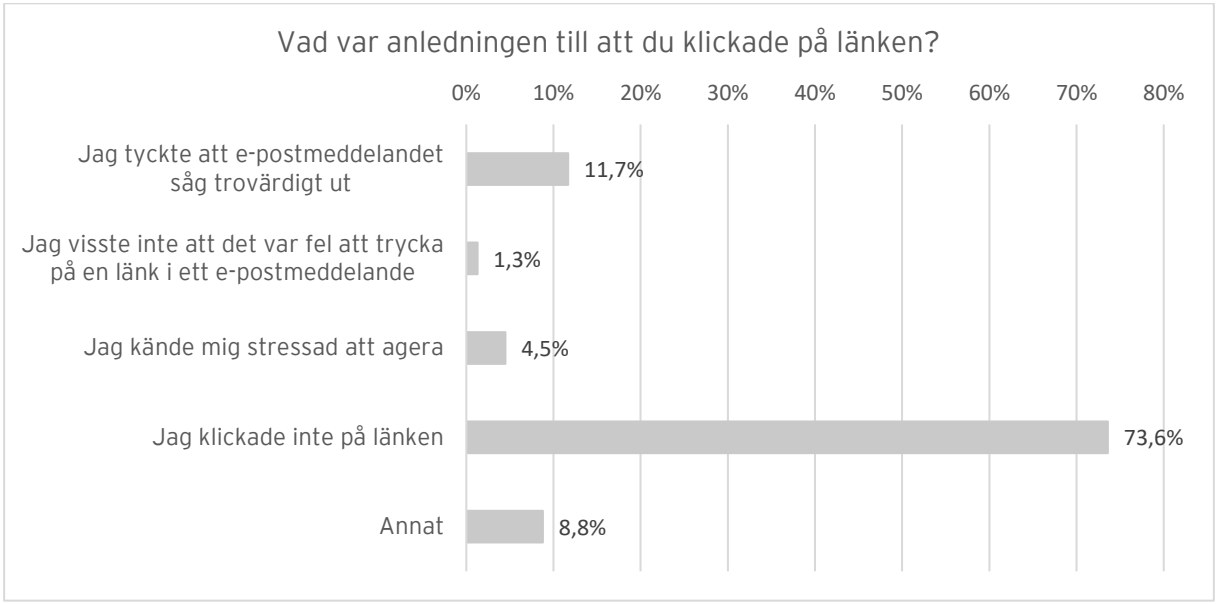
Figur 13 jämför andel mottagare som rapporterade e-postmeddelandet i Tyresö kommun med ett genomsnitt framtaget för jämförbara verksamheter. Figuren visar att Tyresö kommun upplever en lägre andel rapporteringar än jämförbara verksamheter.



Figur 13: Andel mottagare som rapporterade e-postmeddelandet för Tyresö kommun jämfört med ett genomsnitt som baseras på jämförbara verksamheter. I dessa värden inkluderas alla möjliga rapporteringsvägar.

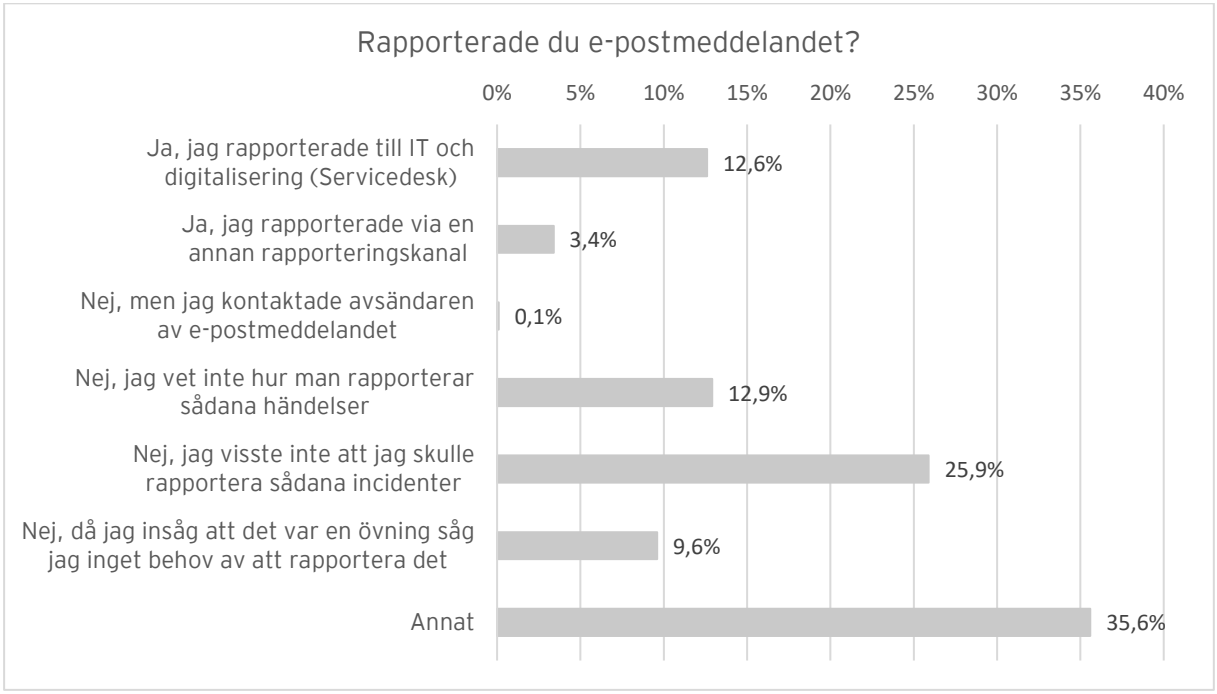
2.3.2 Resultat av enkät

I enkäten som skickades ut efter den genomförda simuleringen deltog 667 medarbetare. Förmågan hos medarbetarna att kunna identifiera falska e-postmeddelanden är av stor vikt för att Tyresö kommun ska kunna minimera riskerna att utsättas för en fullbordad phishing-attack. *Figur 14* 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 (11,7 procent av alla svarande) att de tyckte att e-postmeddelandet såg trovärdigt ut. Fortsättningsvis uppgav 4,5 procent av deltagarna att de klickade på länken för att de upplevde stress att agera i enlighet med e-postmeddelandets uppmaning. Samtidigt uppgav 8,8 procent av mottagarna andra anledningar till att de klickade på länken och endast 1,3 procent att de inte visste att det var fel att trycka på en inbäddad länk i ett e-postmeddelande.



Figur 14: Resultat av enkätfråga om länken i e-postmeddelandet.

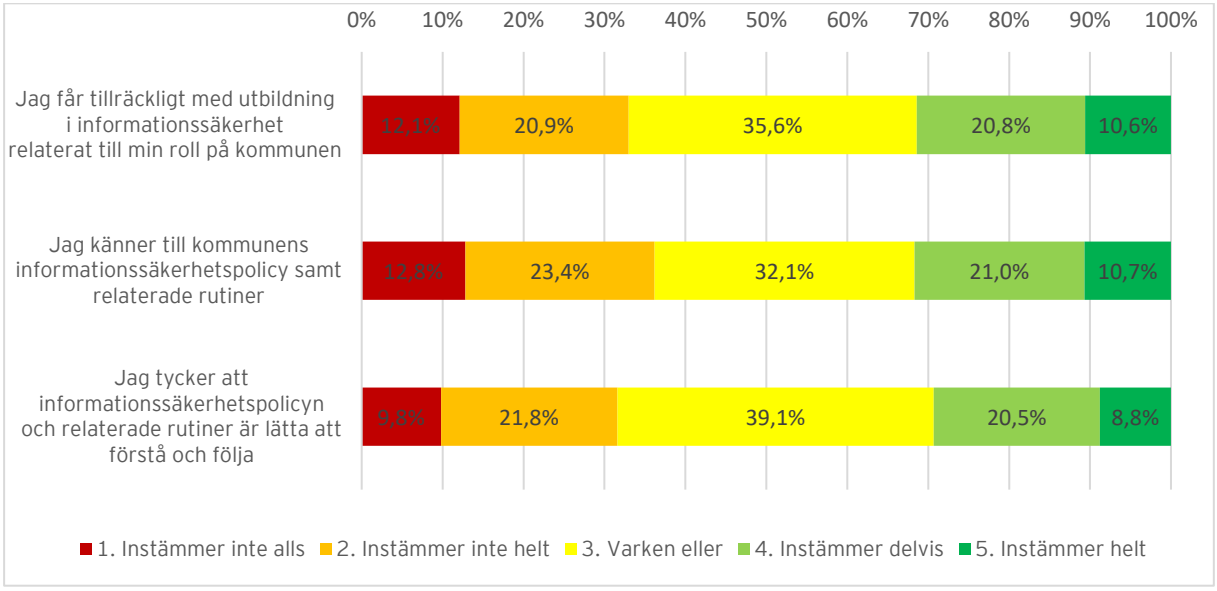
Figur 15 visar huruvida mottagarna valde att rapportera meddelandet eller inte, samt hur och varför. Bortsett från de som uppgav andra anledningar, var det vanligaste svaret som uppgavs av 25,9 procent av alla svarande att de inte visste att ett sådant e-postmeddelande ska rapporteras. Vidare svarade 12,9 procent att de inte vet hur man rapporterar ett falskt e-postmeddelande. Över hälften (51,8 procent) svarade att de inte rapporterade in e-postmeddelandet av olika anledningar. Endast 12,6 procent uppgav att de rapporterade in e-postmeddelandet till Servicedesk, trots att det står specificerat i kommunens informationssäkerhetsinstruktion att det är hit som falska e-postmeddelanden ska rapporteras. Därtill visar enkätresultatet att 3,4 procent rapporterade via en annan rapporteringskanal än Servicedesk. Dessa rapporteringar har dock inte registrerats av kommunen under simuleringen.



Figur 15: Resultat av enkätfråga om mottagarnas rapportering av e-postmeddelandet och anledning bakom beslutsfattandet.

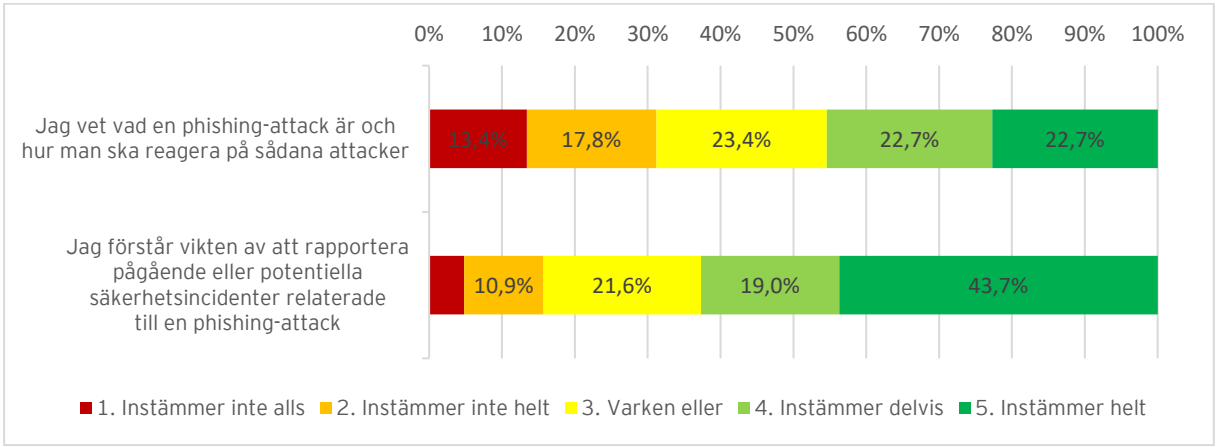
I *figur 16* är mottagarnas svar på frågor relaterade till kommunens styrande dokument, utbildningar och rutiner inom informationssäkerhet samlade. Enkätresultatet utifrån dessa frågor visar att den största andelen av enkätdeltagarna (35,6 procent) uppgav "varken eller" gällande påståendet att de får tillräcklig utbildning inom informationssäkerhet relaterat till sin roll på kommunen. Samtidigt svarade 20,9 procent respektive 12,1 procent att de inte helt och inte alls upplever att de får tillräckligt med utbildning.

Fortsättningsvis svarade 12,8 procent av deltagarna att de inte alls instämmer med påståendet att de känner till kommunens nuvarande informationssäkerhetspolicy och relaterade riktlinjer. 23,4 procent svarade att de inte helt instämmer med påståendet. Den största andelen av deltagarna (32,1 procent) angav "varken eller" på samma påstående. När det kommer till huruvida informationssäkerhetspolicyn och relaterade riktlinjer är lätta att förstå och följa uppgav den största andelen på 39,1 procent av enkätdeltagarna "varken eller". På samma påstående valde 9,8 procent av enkätdeltagarna svarsalternativet "instämmer inte alls" och 21,8 procent "instämmer inte helt".



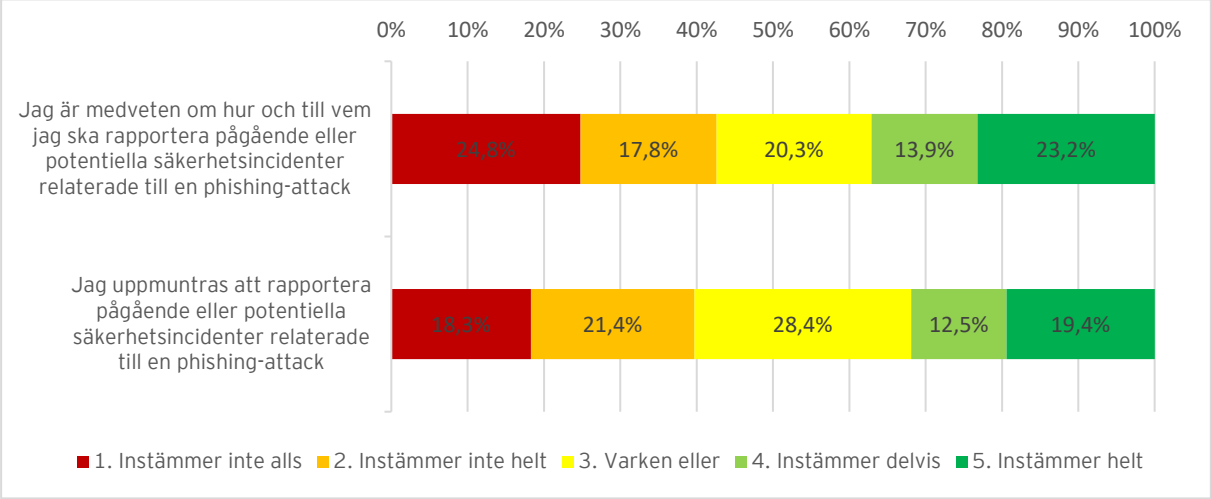
Figur 16: Resultat från påståenden om styrande dokument, utbildning och rutiner inom informationssäkerhet på kommunen.

Figur 17 visar resultatet från enkäten relaterat till medarbetarnas kunskap om vad en phishing-attack är, samt vikten av att rapportera incidenter relaterade till en sådan. Enkätresultaten indikerar att medarbetarna är osäkra på vad en phishing-attack är. 13,4 procent svarade att de inte instämmer alls med påståendet att de vet vad en phishing-attack är och hur man ska reagera om man utsätts för en sådan. Samtidigt svarade 22,7 att de "instämmer helt" och 23,4 procent svarade "varken eller" på samma påstående. Vidare svarade 47,3 procent att de förstår vikten av att rapportera säkerhetsincidenter relaterade till en phishing-attack. 4,8 procent svarade att de inte instämmer alls med påståendet, 10,9 procent att de inte instämmer helt och 21,6 procent svarade "varken eller".



Figur 17: Resultat från påståenden om medarbetarnas kunskap relaterat till phishing-attacker och vikten av att rapportera dessa.

Fortsättningsvis indikerar resultatet från *figur 18* att det råder en viss oklarhet hos enkätdeltagarna kring kommunens rapporteringsrutiner vid säkerhetsincidenter relaterade till en phishing-attack. EY noterar att 24,8 procent av deltagarna anser att de inte vet hur de ska gå till väga och vem de ska kontakta för att rapportera en pågående phishing-attack. Samtidigt uppgav 23,2 procent av enkätdeltagarna att de känner till hur och till vem de ska rapportera en pågående phishing-attack, medan 20,3 procent svarade "varken eller". I relation till detta uppgav 18,3 procent av deltagarna att de inte alls instämmer till påståendet att de uppmuntras av kommunen att rapportera potentiella eller pågående säkerhetsincidenter. Samtidigt instämde 19,4 procent av deltagarna helt till detta påstående och 28,4 procent svarade "varken eller".



Figur 18: Resultat från påståenden om rapportering av phishing-attacker.

3. Övergripande rekommendationer

Baserat på den genomförda analysen bedömer EY att Tyresö kommun ligger på en liknande risknivå som jämförbara kommuner. EY noterar att kommunen som helhet ligger på en medelhög risknivå samt att det finns flera förvaltningar som löper en hög eller mycket hög risk att utsättas för en fullbordad attack. Bedömningen av risken baseras på den typ av verksamhet som bedrivs i Tyresö kommun och på känslighetsgraden av den information som behandlas i den dagliga verksamheten. Således rekommenderar EY kommunstyrelsen att vidta åtgärder för att stärka graden av medvetenhet hos medarbetarna och därmed även motståndskraften mot phishing-attacker. Detta för att undvika förluster av känslig information, negativt rykte eller andra betydande konsekvenser. EY vill betona att det kan räcka med att en medarbetare klickar på en länk i ett falskt e-postmeddelande eller uppger användarinformation för att en cyberkriminell ska ges möjlighet att infiltrera kommunens IT-system. I följande avsnitt presenterar EY tre övergripande rekommendationer som bedöms vara mest relevanta för Tyresö 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 i sin tur 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.

Resultatet av den simulerade phishing-attacken visade på att flera förvaltningar ligger på en hög eller mycket hög risk att utsättas för en fullbordad phishing-attack. Detta innebär att kommunstyrelsens arbete med informationssäkerhet och phishing inte är fullt ut ändamålsenligt, eftersom det kan räcka med att en person klickar på en länk i ett falskt e-postmeddelande för att en cyberkriminell ska kunna ta sig in i kommunens IT-system och/eller komma åt känslig information. EY bedömer att resultatet från simuleringen indikerar att en betydande andel av medarbetarna har låg medvetenhet om phishing och vad som kännetecknar ett sådant e-postmeddelande.

Vidare noterar EY att det i kommunens riktlinjer framgår exempel på vad som kan kännetecknа ett falskt e-postmeddelande samt hur medarbetaren bör agera i situationen. Däremot påvisar resultaten från den utskickade enkäten en viss upplevd otydlighet och ovisshet bland medarbetarna när det kommer till kommunens riktlinjer gällande informationssäkerhet och phishing. EY noterar utifrån enkätresultatet att över 37 procent av medarbetarna inte helt förstår vikten av att rapportera pågående eller potentiella säkerhetsincidenter relaterade till phishing. Samtidigt uppgav 36,2 procent att de inte känner till kommunens informationssäkerhetspolicy och relaterade riktlinjer. Enkäten påvisade även att många medarbetare inom kommunen tycker att kommunens styrdokument relaterat till informationssäkerhet är svåra att förstå.

För att stärka arbetet med informationssäkerhet och phishing inom kommunen rekommenderar EY att kommunstyrelsen säkerställer att befintliga styrdokument och riktlinjer avseende informationssäkerhet och phishing tydligt kommuniceras samt finns tillgängliga för samtliga medarbetare. Detta för att säkerställa att medarbetarna får en bättre kännedom om de befintliga styrdokumenten samt en bättre förståelse för sitt ansvar som medarbetare gällande att vara vaksam och agera på säkerhetsincidenter.

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 säkerställa att effektiva rapporteringsvägar existerar samt att medarbetare är medvetna om hur och när dessa ska användas. Då medarbetare tenderar att agera på ett falskt e-postmeddelande direkt vid upptäckt är det av betydelse att medarbetare rapporterar händelsen direkt om misstanke finns. Detta så att organisationens incidenthantering kan aktiveras i tid innan fler medarbetare hinner agera på det falska e-postmeddelandet i enlighet med vad som uppmanas av avsändaren. Effektiva rapporteringsvägar samt medvetenhet om dessa kan därför möjliggöra identifiering av eventuella hot och att nödvändiga åtgärder kan tas inom skälig tid.

Enligt kommunens informationssäkerhetsinstruktion, som nås på kommunens intranät, ska medarbetare vid upptäckt av misstänka e-postmeddelanden rapportera detta till Servicedesk. EY noterar att kommunen har en låg grad av rapporteringar i jämförelse med jämförbara verksamheter då endast 2,3 procent av medarbetarna rapporterade e-postmeddelandet under simuleringen. Detta kan innebära en risk i form av att IT-avdelningen underskattar omfattningen av phishing-attacken eller inte hinner reagera i tid.

I informationssäkerhetsinstruktionen framgår det även att Servicedesk ska kontaktas via kommunens IT-portal som nås via kommunens intranät. Av de rapporteringar som registrerades till Servicedesk var det dock endast 4,7 procent som gjordes via IT-portalen. 76,7 procent av de som rapporterade e-postmeddelandet gjorde i stället detta via e-post och 18,6 procent via telefon. Detta indikerar att den föredragna rapporteringsvägen var den som i praktiken användes minst av medarbetarna. Enligt enkäten var det också 3,4 procent av medarbetarna som använde en annan rapporteringskanal än Servicedesk. Detta har däremot inte fångats upp av kommunen under simuleringen. EY rekommenderar således att kommunstyrelsen säkerställer att den föredragna rapporteringsvägen förtydligas samt kommuniceras till samtliga medarbetare. Detta eftersom det vid en pågående phishing-attack är avgörande att kommunens incidenthantering aktiveras.

Resultatet av granskningen indikerar även att medarbetarnas medvetenhet om befintliga rapporteringsvägar för säkerhetsincidenter relaterade till phishing är låg. Exempelvis var 25,9 procent av enkätdeltagarna inte medvetna om att falska e-postmeddelanden ska rapporteras. Därtill uppgav 24,8 procent av enkätdeltagarna att de inte var medvetna om hur de ska gå till väga eller vem de ska kontakta för att rapportera en pågående eller misstänkt phishing-attack. EY noterar även att flertalet medarbetare känner sig osäkra på

om de av kommunen har blivit uppmuntrade till att rapportera incidenter relaterade till phishing. EY rekommenderar därför kommunstyrelsen att säkerställa en tydligare kravställning avseende medarbetarens ansvar gällande rapportering av misstänka e-postmeddelanden, samt säkerställa att vikten av att rapportera misstänkta e-postmeddelanden kommuniceras till samtliga medarbetare. Detta för att öka möjligheten för kommunen att reagera på en misstänkt phishing-attack i tid.

3.3 Teoretiska och praktiska utbildningar inom phishing

I takt med att mängden cyberattacker mot organisationer har ökat generellt under de senaste åren har EY noterat en markant ökning specifikt i antalet phishing-attacker. En förklaring till detta är bland annat förändrade arbetssätt som inneburit en ökad användning av digitala verktyg. Medarbetares medvetenhet och kunskap om informationssäkerhet blir således allt viktigare för att säkerhetsställa ett adekvat skydd av informationen hos en organisation. Sådan kunskap innefattar bland annat vad phishing är, hur falska e-postmeddelanden kan upptäckas samt konsekvenserna av en fullbordad phishing-attack.

Simuleringen samt medföljande enkät har påvisat att det finns en ovisshet bland medarbetarna när det gäller vad phishing är, vilket ansvar medarbetaren har, samt vilka konsekvenser en fullbordad phishing-attack kan resultera i. Ur enkätresultatet framgår det att 33 procent av medarbetarna upplever att de inte får tillräckligt med utbildning i informationssäkerhet relaterat till sin roll på kommunen. EY rekommenderar således kommunstyrelsen att säkerställa att utbildningar inom informationssäkerhet och phishing erbjuds. EY rekommenderar även att viss utbildning fokuserar på hur falska e-postmeddelanden, domäner och hemsidor kan identifieras. Därtill rekommenderar EY att det i erbjudna utbildningar ska finnas utrymme för diskussioner och möjlighet till övning för att identifiera phishing-attacker. Detta för att öka medvetenheten bland medarbetarna och minska risken för kommunen att utsättas för en fullbordad phishing-attack.

Resultaten från simuleringen visar även att medvetenheten kring phishing och medarbetarens ansvar varierar inom olika förvaltningar. Bland annat tyder resultaten på att den politiska organisationen har en mycket hög risk att agera på en phishing-attack i enlighet med vad den cyberkriminella aktören uppmanar till. EY rekommenderar således kommunstyrelsen att säkerställa riktade och målgruppsanpassade utbildningsinsatser för att fokusera på förvaltningar med högre risk både på grund av en lägre medvetenhet om phishing-attacker, men även med hänsyn till den information som behandlas i förvaltningen. Detta för att säkerställa att medarbetare som är verksamma i de delar av kommunen där känslig information behandlas erbjuds utbildning inom phishing och informationssäkerhet.

EY rekommenderar även att kommunstyrelsen säkerställer att utbildningar följs upp med regelbundna tester av säkerhetsmedvetenhet och kunskap inom phishing hos medarbetarna. Detta för att kontrollera effekten av genomförda utbildningsinsatser, fortsätta sprida kunskapen inom kommunen samt kontinuerligt testa medarbetarnas kunskap och medvetenhet i praktiken. Tillvägagångssätt som kan tillämpas inom kommunen är förslagsvis interaktiva utbildningsmaterial och nätbaserade simuleringar.

4. Revisionsfrågor

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

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

Revisionsfråga	Svar	
▸ Hanterar Tyresö kommuns medarbetare hotet från attacker genom falska email, så kallad phishing (nätfiske), på ett ändamålsenligt sätt?	Tyresö kommuns medarbetare bedöms delvis hantera hotet från attacker genom falska e-postmeddelanden på ett ändamålsenligt sätt. Bedömningen baseras på att kommunen har vidtagit åtgärder för att minska risken för phishing, men ändå inom flera förvaltningar löper en hög risk att utsättas för en fullbordad phishing-attack. Det bör betonas att det kan räcka med att *en användare* uppger användarnamn och lösenord för att en angripare ska ges möjlighet att ta sig in i kommunens IT-miljöer. Baserat på den genomförda granskningen bedömer EY att Tyresö kommun bör arbeta för att förbättra sin motståndskraft mot phishing med avseende på medarbetarnas hantering av en phishing-attack. Slutsatsen är att kommunstyrelsen delvis har säkerställt att Tyresö kommuns medarbetare hanterar hot från phishing-attacker på ett ändamålsenligt sätt.	
▸ Har Tyresö kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av de testade medarbetarna under den simulerade attacken?	EY bedömer att incidenthanteringsprocessen inte aktiveras på ett ändamålsenligt sätt. Tyresö kommun har en informationssäkerhetsinstruktion som uppmanar till att rapportering ska ske vid misstanke om falska e-postmeddelanden och att denna ska ske till Servicedesk via deras IT-portal som kan hittas på intranätet.	

	Däremot rapporterade endast 2,3 procent av medarbetarna incidenten, vilket ligger under genomsnittet för jämförbara verksamheter. Av de som rapporterade meddelandet var det endast 4,7 procent som gjorde detta i enlighet med den önskvärda rapporteringsväg som specificerats i riktlinjerna. Detta indikerar att det finns en osäkerhet bland medarbetarna gällande hur de ska rapportera incidenter relaterade till phishing. En sådan osäkerhet kan leda till att medarbetarna inte rapporterar e-postmeddelandet och därmed en ineffektiv incidenthantering. Om ytterligare önskvärda rapporteringsvägar existerar borde även dessa specificeras i kommunens riktlinjer. Därmed bedömer EY att kommunstyrelsen inte har möjliggjort för medarbetarna att på ett ändamålsenligt sätt aktivera incidenthanteringsprocessen.	
► Är riktlinjer för hantering och rapportering av falska email och andra incidenter kända hos medarbetarna?	EY bedömer att kommunens riktlinjer för hantering och rapportering av falska e-postmeddelanden inte är kända hos medarbetarna. I Tyresö kommun finns dokumenterade riktlinjer och rutiner för hur medarbetarna ska hantera ett förmodat falskt e-postmeddelande vid en phishing-attack. Dessa riktlinjer finns tillgängliga för samtliga medarbetare på kommunens intranät. Granskningen visar däremot att medarbetarna i stor utsträckning uppger att riktlinjerna är svåra att förstå, och att många medarbetare inte känner till dem. Därutöver visar enkätresultatet att en betydande andel av medarbetarna inte vet att de ska rapportera en pågående phishing-attack eller hur de ska gå till väga. Detta försvårar för kommunen att upprätthålla en god beredskap och effektivt agerande vid en pågående phishing-attack. Således bedömer EY att kommunstyrelsen inte har kommunicerat instruktioner, rutiner och riktlinjer för informationssäkerhet till medarbetarna på ett tillfredsställande sätt.	

5. Slutsatser

Granskningen syftade till att undersöka om kommunstyrelsen hos Tyresö kommun säkerställt en tillräcklig intern kontroll med avseende på kommunens praktiska arbete med IT- och informationssäkerhet inom området phishing. Genom en simulerad phishing-attack samt medföljande enkät har EY undersökt utbildning och medvetenhet hos medarbetarna.

Den genomförda granskningen svarar på följande revisionsfrågor:

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

Resultatet visar att Tyresö kommun har flera förvaltningar som ligger på en hög risk att utsättas för en fullbordad phishing-attack. EY noterar 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 visar resultaten att få anställda rapporterade incidenten och ännu färre rapporterade enligt kommunens riktlinjer. Fortsättningsvis visar även enkätresultatet 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, för att få en effektiv och samlad rapportering. Kommunstyrelsen rekommenderas även att stärka utbildning och medvetenheten hos medarbetarna om phishing och hur de kan upptäcka ett falskt e-postmeddelande.

Baserat på resultatet från granskningen har EY valt att presentera följande tre övergripande rekommendationer som Tyresö 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.
- Genomför teoretiska och praktiska utbildningar inom phishing.

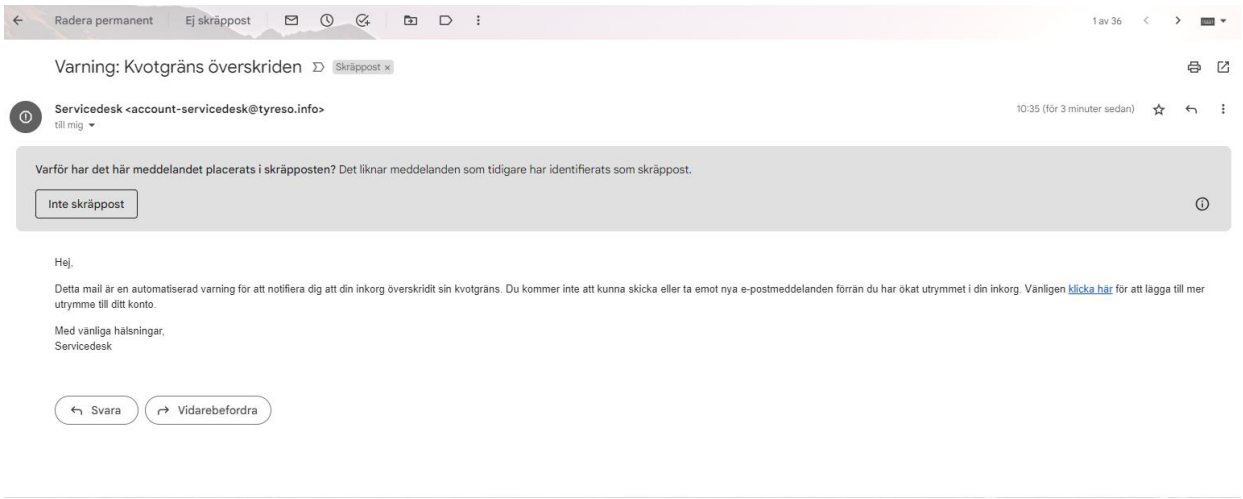
Stockholm, 2023-09-10

Helena Törnqvist

Partner, EY

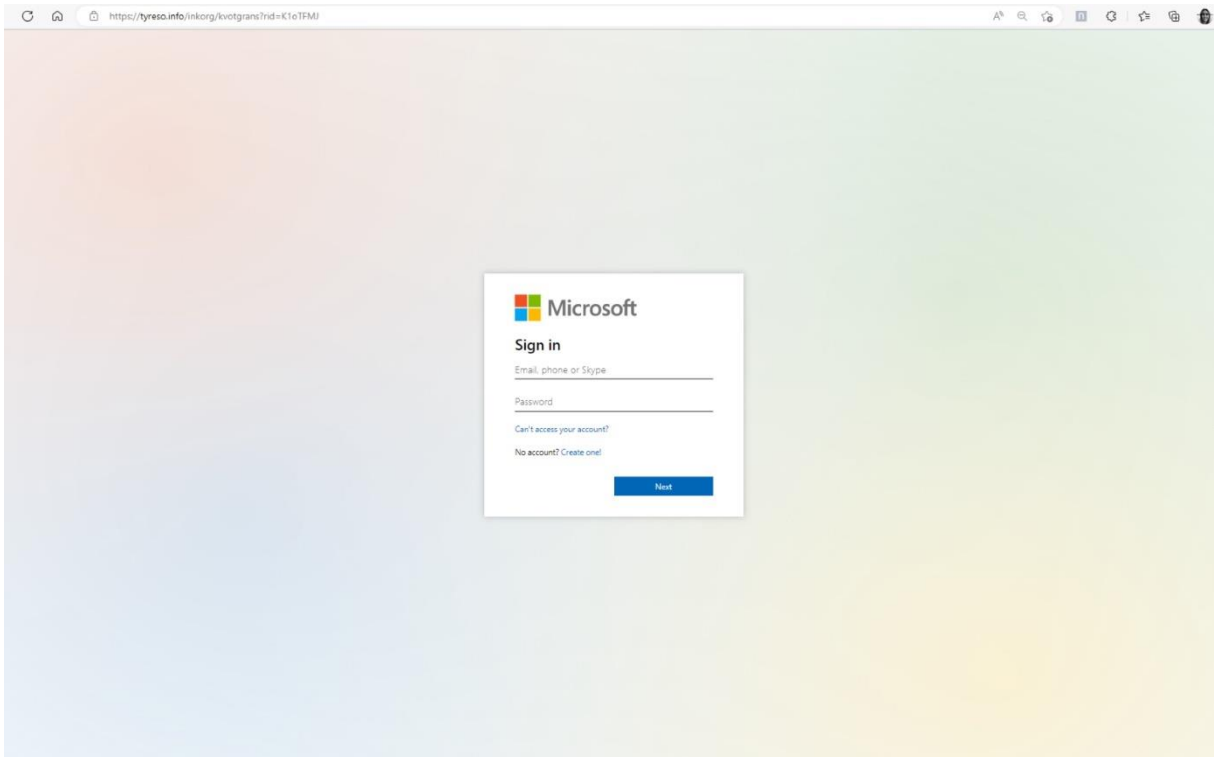
Bilaga 1: E-postmeddelande

E-postmeddelande

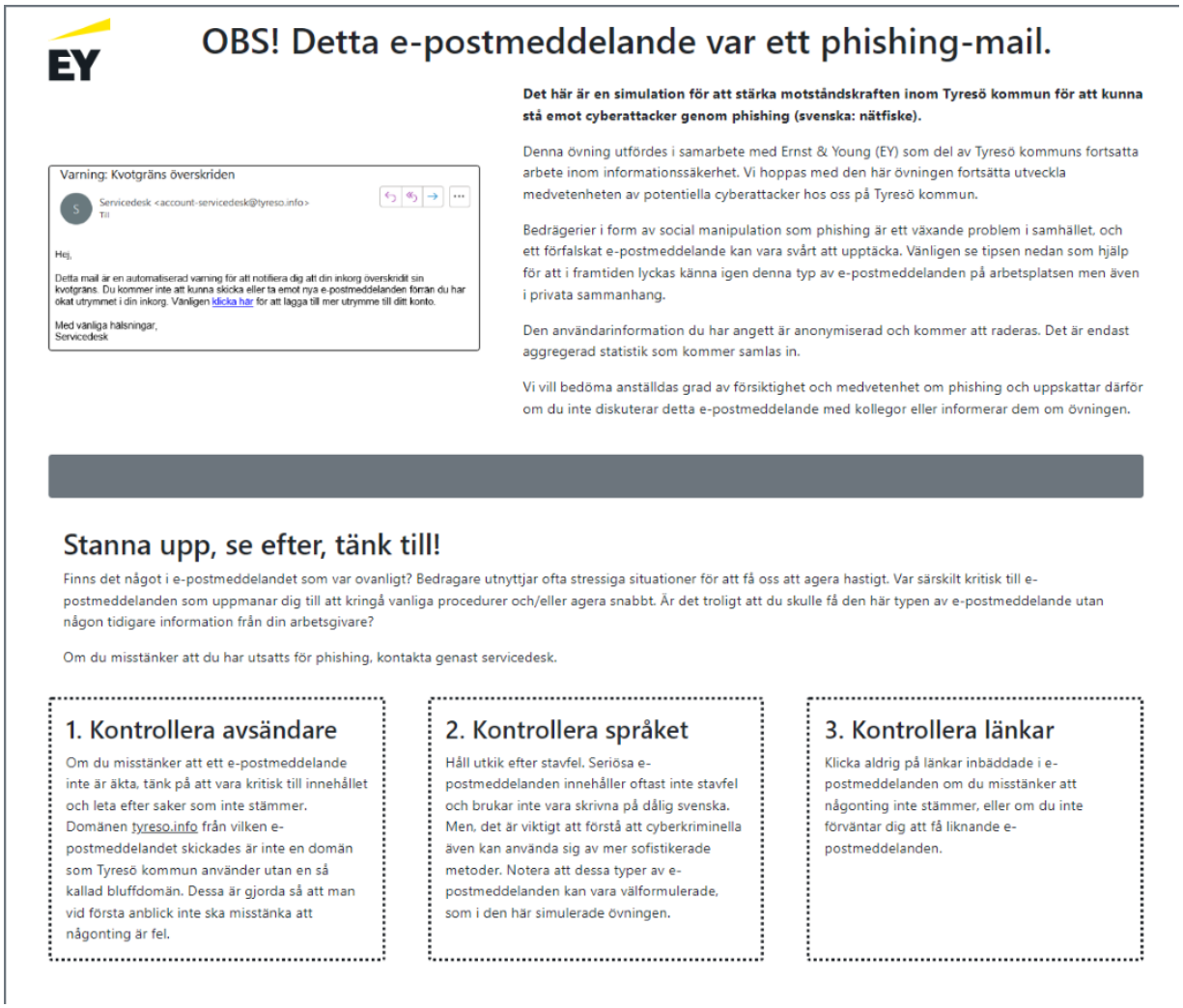


Bilaga 2: Landningssida

Landningssida 1



Landningssida 2



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

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

Varning: Kvotgräns överskriden

Servicedesk <account-servicedesk@tyreso.info>
Till

Hej,

Detta mail är en automatiserad varning för att notifiera dig att din inkorg överskridit sin kvotgräns. Du kommer inte att kunna skicka eller ta emot nya e-postmeddelanden förrän du har ökat utrymmet i din inkorg. Vänligen klicka här för att lägga till mer utrymme till ditt konto.

Med vänliga hälsningar,
Servicedesk

Denna övning utfördes i samarbete med Ernst & Young (EY) som del av Tyresö kommuns fortsatta arbete inom informationssäkerhet. Vi hoppas med den här övningen fortsätta utveckla medvetenheten av potentiella cyberattacker hos oss på Tyresö kommun.

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 men 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, 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 till att kringå vanliga procedurer och/eller agera 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 tyreso.info från vilken e-postmeddelandet skickades är inte en domän som Tyresö 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-postmeddelanden 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	Medelhög 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 rutiner, och 3) Rapportering. Följande frågor besvaras på en skala enligt nedan:

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

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

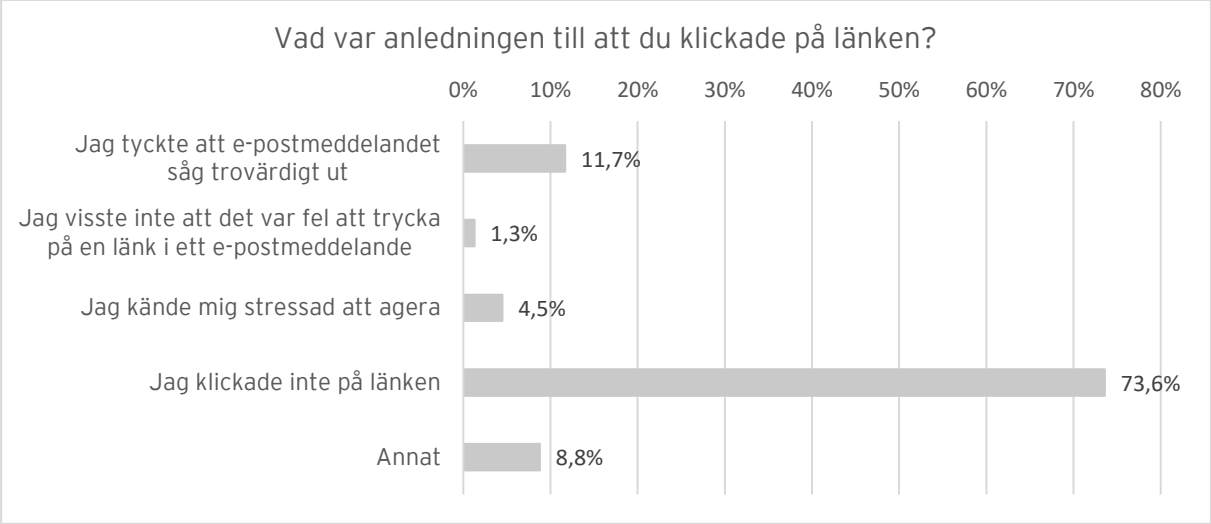
Policy och riktlinjer

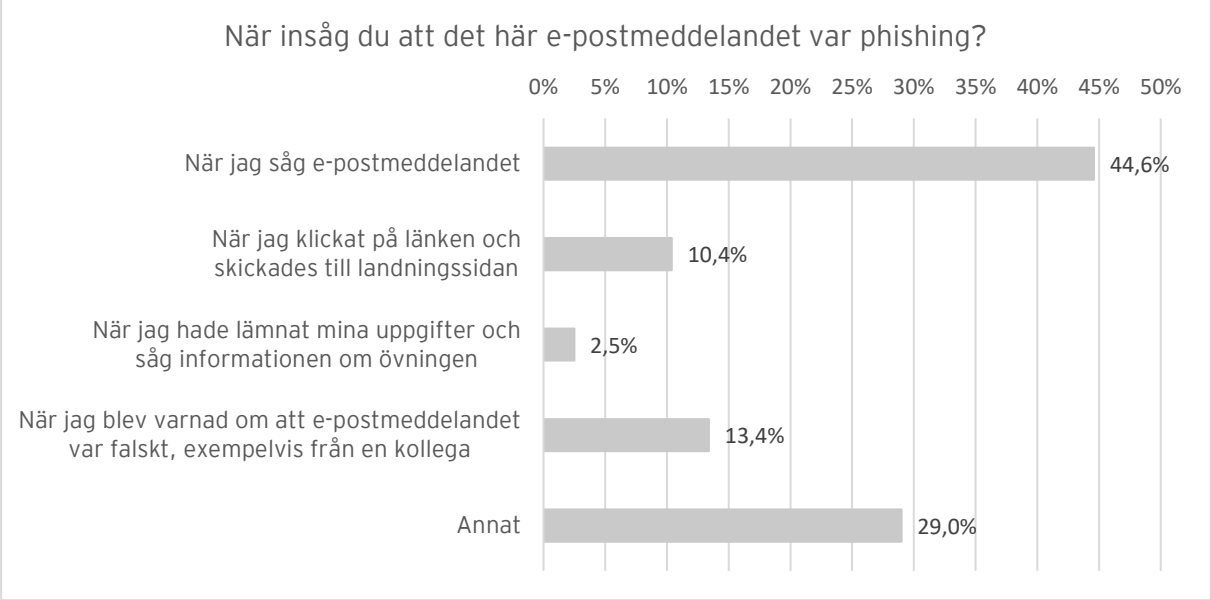
- Jag känner till kommunens informationssäkerhetspolicy samt relaterade rutiner
- Jag tycker att informationssäkerhetspolicyn och relaterade rutiner är lätta att förstå och följa
- Jag är medveten om de potentiella hot och negativa konsekvenser som kan uppstå av att inte efterleva kommunens policyer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

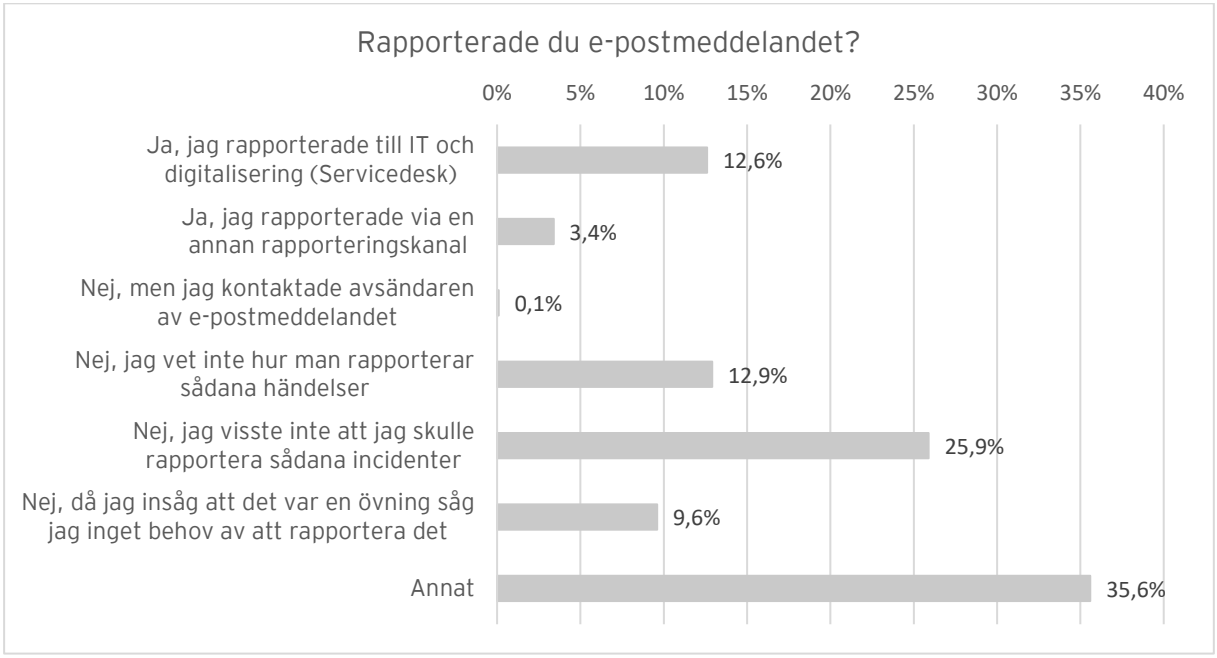
Rapportering

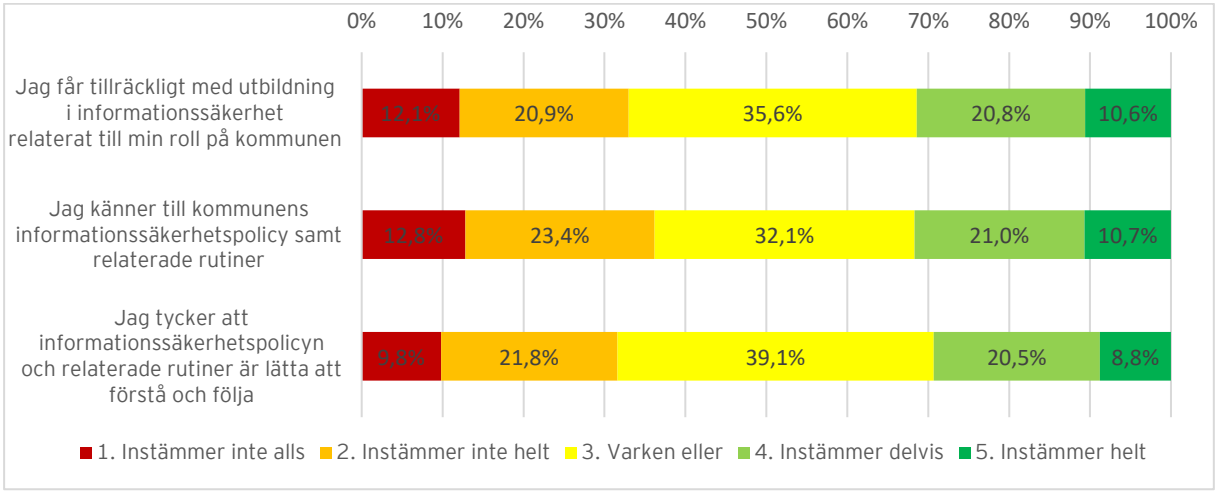
- Jag förstår vikten av att rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack
- Jag uppmuntras att rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack
- Jag är medveten om hur och till vem jag ska rapportera pågående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

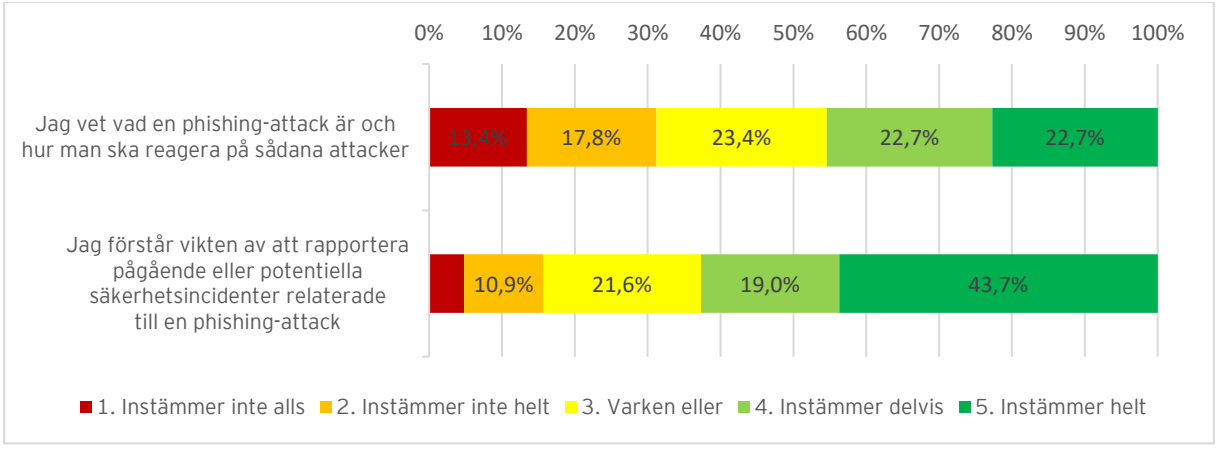
Bilaga 5: Enkätresultat

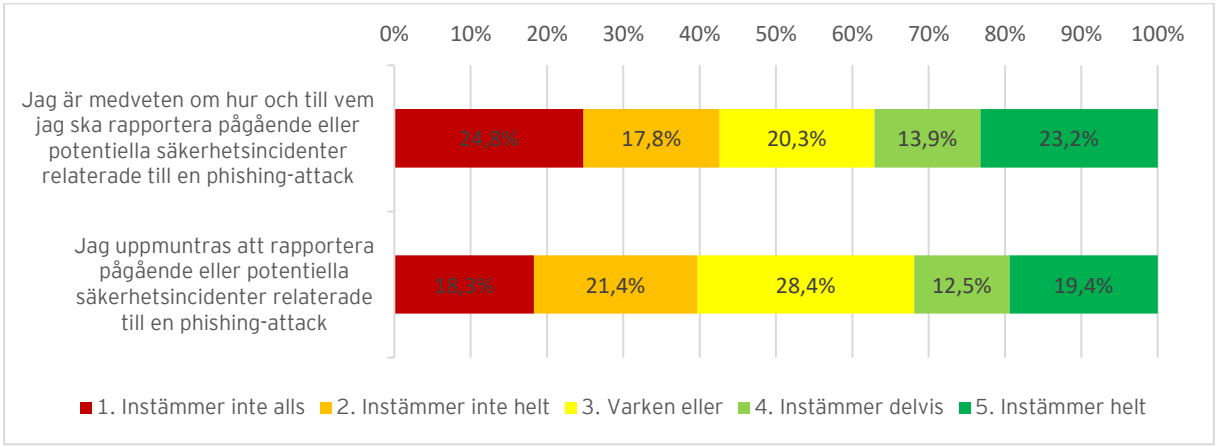


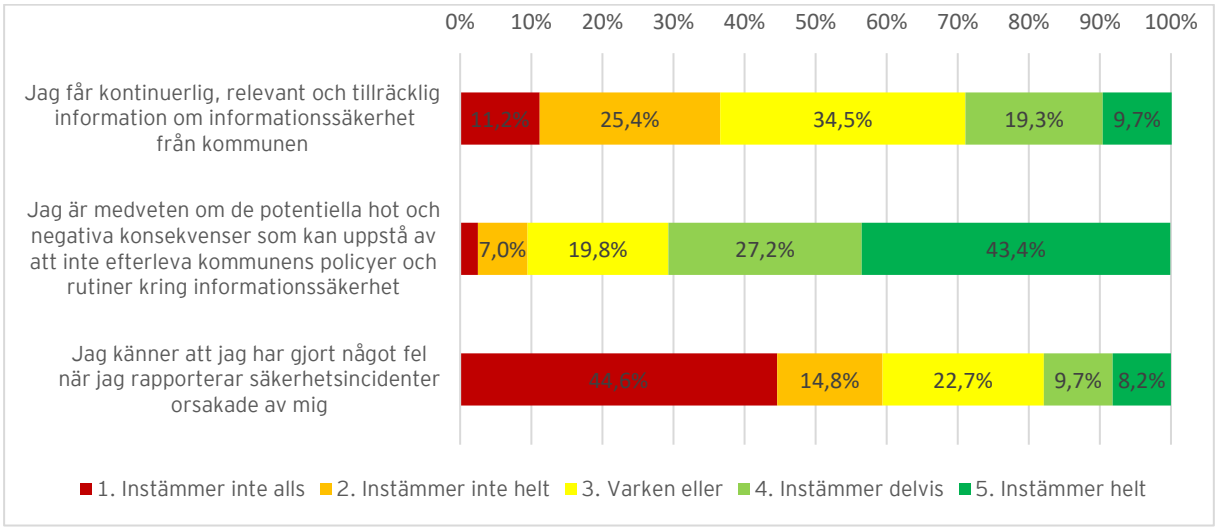



Rapporterade du e-postmeddelandet?
0%
5%
10%
15%
20%
25%
30%
35%
40%
Ja, jag rapporterade till IT och digitalisering (Servicedesk)
12,6%
Ja, jag rapporterade via en annan rapporteringskanal
3,4%
Nej, men jag kontaktade avsändaren av e-postmeddelandet
0,1%
Nej, jag vet inte hur man rapporterar sådana händelser
12,9%
Nej, jag visste inte att jag skulle rapportera sådana incidenter
25,9%
Nej, då jag insåg att det var en övning såg jag inget behov av att rapportera det
9,6%
Annat
35,6%


0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Jag får tillräckligt med utbildning i informationssäkerhet relaterat till min roll på kommunen
12,1%
20,9%
35,6%
20,8%
10,6%
Jag känner till kommunens informationssäkerhetspolicy samt relaterade rutiner
12,8%
23,4%
32,1%
21,0%
10,7%
Jag tycker att informationssäkerhetspolicyn och relaterade rutiner är lätta att förstå och följa
9,8%
21,8%
39,1%
20,5%
8,8%
1. Instämmer inte alls
2. Instämmer inte helt
3. Varken eller
4. Instämmer delvis
5. Instämmer helt


0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Jag vet vad en phishing-attack är och hur man ska reagera på sådana attacker
13,4%
17,8%
23,4%
22,7%
22,7%
Jag förstår vikten av att rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack
10,9%
21,6%
19,0%
43,7%
1. Instämmer inte alls
2. Instämmer inte helt
3. Varken eller
4. Instämmer delvis
5. Instämmer helt


0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Jag är medveten om hur och till vem jag ska rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack
24,8%
17,8%
20,3%
13,9%
23,2%
Jag uppmuntras att rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack
18,3%
21,4%
28,4%
12,5%
19,4%
1. Instämmer inte alls
2. Instämmer inte helt
3. Varken eller
4. Instämmer delvis
5. Instämmer helt


0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Jag får kontinuerlig, relevant och tillräcklig information om informationssäkerhet från kommunen
11,2%
25,4%
34,5%
19,3%
9,7%
Jag är medveten om de potentiella hot och negativa konsekvenser som kan uppstå av att inte efterleva kommunens policyer och rutiner kring informationssäkerhet
7,0%
19,8%
27,2%
43,4%
Jag känner att jag har gjort något fel när jag rapporterar säkerhetsincidenter orsakade av mig
44,6%
14,8%
22,7%
9,7%
8,2%
1. Instämmer inte alls
2. Instämmer inte helt
3. Varken eller
4. Instämmer delvis
5. Instämmer helt

Bilaga 6: 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 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 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 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.

Bilaga 7: Förteckning över använda bilagor

- 2023 KS 0166 – Informationssäkerhetsinstruktion.pdf